Infoblox

Q3 | 2022 CYBER THREAT REPORT

Powered by the
Infoblox Threat Intelligence Group

Disclaimer

Infoblox publications and research are made available solely for general information purposes. The information contained in this publication is provided on an “as is” basis. Infoblox accepts no liability for the use of this data. Any additional developments or research since the date of publication will not be reflected in this report.

Table of Contents

Executive Summary **4**
Introducing the Infoblox Reputation Scoring Capability **4**
Baselining Reputation Scores for TLDs in Anonymized Infoblox Customer Traffic 4
Value of and Need for a Scoring Algorithm 5
Algorithm Overview 5
TLD Reputation Scoring 6
Future Directions 11
Emotet: A Malware Family That Keeps Going **11**
Executive summary 11
Emotet delivery vehicles 12
File attachments analysis 13
Malicious payloads domain distribution 14
Analysis of C&C infrastructure 16
Emotet's global footprint 16
Prevention and mitigation 18
Indicators of compromise 18
Omnatuor Malvertising Network Hijacks Browser Settings to Spread Riskware **24**
Summary 24
Discovery 24
Infrastructure 26
Attack Chain 26
Attack Chain: Initial Access 27
Attack Chain: Execution 28
Attack Chain: Persistence 29
Recommendations and Mitigation 30
Indicators of Compromise 30
CISA Alerts: Q3 2022 ..... **31**
FBI IC3 Industry Alerts: Q3 2022 ..... **37**
National Security Agency/Central Security Service (NSA-CSS) Advisries and Guidance: Q3 2022 ..... **37**
Control System Defense: Know the Opponent 37
The Infoblox Threat Intelligence Group **44**
Infoblox Threat Intelligence **44**

Executive Summary

We at Infoblox are pleased to publish this Q3 2022 edition of our Quarterly Cyber Threat Intelligence Report. We publish these reports during the first month of each calendar quarter.

This Q3 2022 report puts a special and introductory spotlight on the Infoblox Threat Intelligence Group's (TIG) original research into Top Level Domain (TLD) Reputation Scoring and on how this information can help organizations assess potential threats. This is the first time we have released and published this data externally to such a broad audience. The team expects to be updating this original research on a quarterly basis.

This report includes information on industry alerts, advisories, reports and original research published from July 1 to September 30, 2022, by the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and the NSA/CSS (National Security Agency Central Security Service).

This publication supplements our original research and insight into threats we observed leading up to and including this period of time. We feel that timely information on cyber threats is vital to protecting the community at large.

Introducing the Infoblox Reputation Scoring Capability

Baselining Reputation Scores for TLDs in Anonymized Infoblox Customer Traffic

Classifying the reputation or risk of internet infrastructure is essential to the effective defense of an organization's network. Defenders have limited resources and must focus on threats that pose the highest risk to their organization. Although there have been many attempts to develop algorithms that can produce classification scores, most produce scores that are challenging to interpret and use for comparison purposes. Infoblox researchers recently developed a new scoring algorithm that addresses both of these challenges. To introduce the algorithm and demonstrate its usefulness, Infoblox researchers applied it to the past six months of anonymized DNS data from our resolvers to determine the reputation, or risk, associated with `com`, `net`, and other top level domains (TLDs) that appeared in the traffic. With high confidence, the researchers classified ten TLDs as high-risk, meaning that these TLDs were more likely to contain malicious domains than other TLDs were: `bid`, `cam`, `cfd`, `click`, `icu`, `ml`, `quest`, `rest`, `top`, and `ws`.

Using this algorithm to classify the risk of TLDs is just the first step. In later quarterly reports, we will show how it can be used to classify internet infrastructure elements such as nameservers and domain registrars. In the future, we will also explore how the results of these investigations can be used by our customers to evaluate and prioritize potential threats to their networks.

Value of and Need for Scoring Algorithm

Ranking and comparing threats can be very complicated, especially given the shifting landscape of cybersecurity from day to day. Therefore, having a robust, quantifiable, and repeatable process for scoring large amounts of data can be invaluable as defenders prioritize their limited resources for securing systems and analyzing their traffic and alerts. While there have been a number of attempts at creating such an algorithm, with the most recent notable attempt by Spamhaus, most fall short of producing scores that can be interpreted by a wide variety of audiences and can be easily used to provide meaningful comparisons. In response to this need, researchers from Infoblox's Threat Intelligence Group developed a generic scoring algorithm that can be applied to data from TLDs, nameservers, and other objects.

Algorithm Overview

Our new reputation-scoring algorithm uses only two pieces of information: the total number of observations and the number of observations meeting a specific criteria. When we apply our algorithm to TLDs to generate risk scores, the values are the total number of observed domains in the TLD and the number of observed malicious domains in the TLD. Using these two values, the algorithm produces a score from zero to ten: that is, `[0:10]`. A score of 5 is interpreted as the normal, expected score and is classified as "moderate risk". The scores of 4 and 6 are close enough that they are also classified as "moderate risk". In the case of TLDs, this means that we would expect any randomly selected TLD to have a score of 5. For example, the TLD `com` had a score of 5 in August, because it had an average number of malicious domains relative to the total number of observed domains in the TLD (see the highlighted point in the Moderate Risk range in Figure 1). Scores below 5 have a lower-than-average score (that is, a lower-than-average percentage of malicious domains), while scores above 5 have a higher-than-average score (that is, a higher-than-average percentage of malicious domains).

Exact scores are calculated using the data's standard deviation, which indicates how far away from the average a given item is. A low standard deviation means that most of the data is close to the average, while a high standard deviation means that the data is spread out. In our case, a score of 4 indicates that the item is one standard deviation less than the average, while a score of 6 is one standard deviation more than the average, as shown below. One would expect 68% of all data to be in this range, which is why these scores are referred to as the moderate, expected risk of a TLD. A score of 3 is two standard deviations less than the average, and so on. These scores mean that the TLDs are either much less risky or much more risky than the average. For example, the TLD `edu` had a score of 3 in August, meaning we observed it to have far fewer malicious domains than average; on the other hand, the TLD `click` had a score of 7, meaning we observed it to have far more malicious domains than average (see the highlighted points in the Low Risk and High Risk ranges in Figure 1).

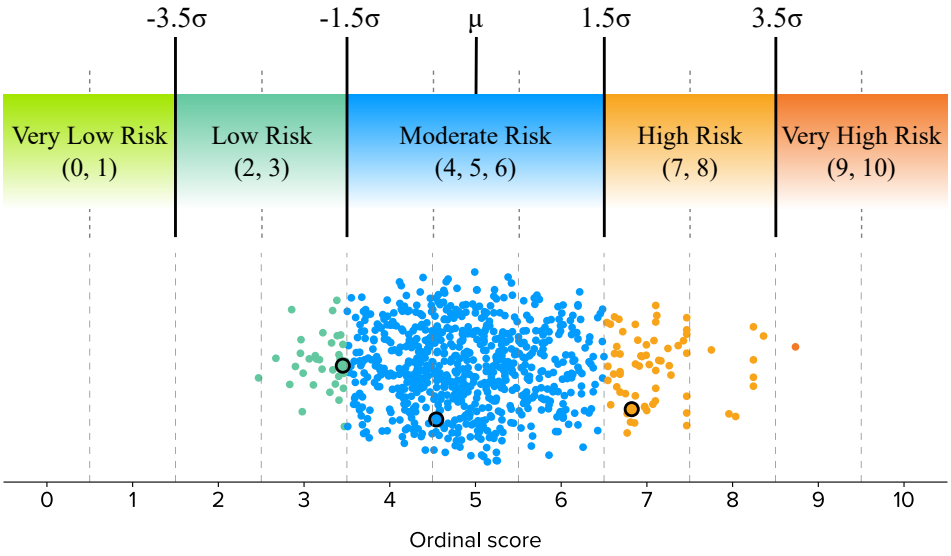


Figure 1: Scores are assigned based on a TLD's standard deviation (denoted σ) from the mean value (denoted μ). One can think of the TLD's standard deviation as being rounded to the nearest whole number in order to calculate the ordinal score, as shown here. Scores with values of 4, 5, and 6 are classified as *moderate risk*, which is the score one would expect for a normal TLD. Scores higher than that are classified as *high risk*, while lower scores are classified as *low risk*. Raw TLD scores from August are shown here with the TLDs `edu`, `com`, and `click`, highlighted in the low, moderate, and high risk categories, respectively.

While the algorithm is robust to the inevitable limitations of what we can observe, sometimes those limitations are extreme. In some cases, we may not observe any malicious domains for a TLD; in other cases, we may observe only malicious and no benign domains for a TLD. In these situations, we assign scores of 0 and 10, respectively. Also, we most likely will assign a low confidence score to each TLD, to indicate this uncertainty in the overall score. The algorithm is also robust to differences in the number of observations between TLDs. For example, the number of domains in the TLD `com` is vastly greater than the number of domains in most other TLDs. Even so, the risk scores between all the TLDs can be used for comparison, regardless of the differences in the number of observed domains.

The calculated scores can then be used to classify the TLD being scored into five distinct risk categories: Very Low Risk, Low Risk, Moderate Risk, High Risk, and Very High Risk (see Figure 1).

TLD Reputation Scoring

Infoblox researchers chose TLDs for the first application of our new reputation-scoring algorithm. We gathered data for the previous two quarters (April through June and July through September) and calculated scores for each observed TLD for each month. Figure 2 illustrates the distribution of TLD scores for the month of September. The vast majority of TLDs were assigned a risk score of 0, which is the lowest risk score possible. As previously mentioned, a TLD is assigned a score of 0 if no malicious domains are observed for it. Most of these 0 scores are due to the fact that only a few domains were observed in the TLD (fewer than ten), and this resulted

in low confidence in the score. For example, the TLD `cc.ok.us` is reserved for community colleges in the state of Oklahoma. There were only a handful of domains in the TLD, and none of them were classified as malicious. This doesn't mean that there were no malicious domains in the TLD; it simply means none were observed. As a result, the TLD was assigned a score of zero and low confidence.

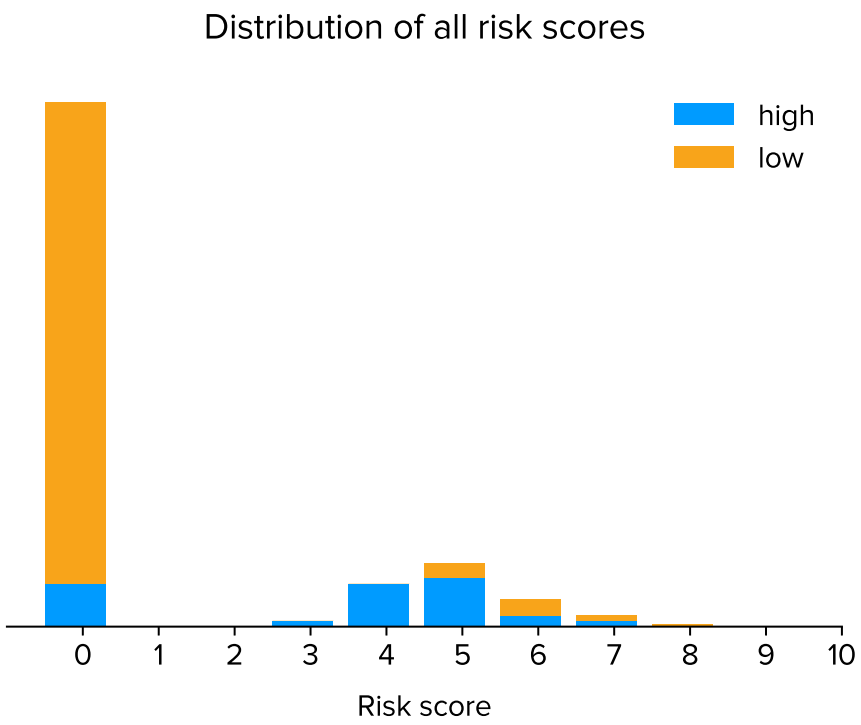


Figure 2: The distribution of risk scores for all TLDs observed during September. Scores are broken out by the algorithm's confidence in the calculated score.

Not all 0 scores are assigned with low confidence, however. Figure 3 shows the distribution of only high-confidence scores, and it includes quite a few 0 scores. Again, this is due to the fact that no malicious domains were observed in the TLD. In these cases, however, there were enough benign domains observed in the TLD that the algorithm had a high confidence in the score, and this again highlights the algorithm's reliance on quality and breadth of the observation data. For example, the TLD `gov.cn` is reserved for Chinese government websites. The TLD has thousands of domains, none classified as malicious; this resulted in a risk score of 0. However, because there were so many observed domains, there is high confidence in the score. Setting aside these TLDs with a score of 0, the score distribution of the remaining TLDs is somewhat normal, about the expected risk score of 5, as is anticipated.

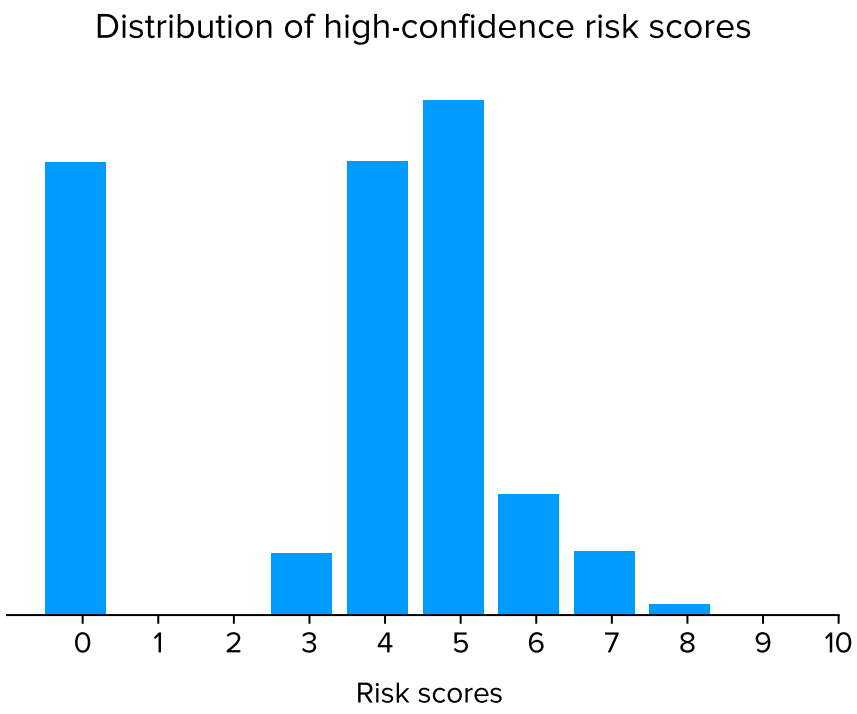


Figure 3: The distribution of TLD risk scores that were observed during September and for which the algorithm has high confidence.

In contrast to the numerous TLDs with a score of 0, very few TLDs were assigned a score of 10, which indicates that all observed domains in the TLD were malicious. As one would expect, such score assignments are very rare. Researchers have seen only a few TLDs with a score of 10, and only one of them has high confidence.

Given the ever-changing landscape of the web, TLD scores depend on the observations used in calculations and will change over time as new observations are made. To improve confidence in scoring and risk classification, we assessed TLDs for consistency before selecting them for further analysis. The most consistently high-risk TLDs across the previous and current quarters, totalling six months, are shown in Table 1 below. Given the highly variable nature of the internet, sensing capabilities, and threat actor infrastructure, it is not uncommon for a TLD's risk score to vary from month to month. As a result, a TLD being consistently classified as high risk indicates a long-term risk that warrants action by defenders. While not every domain in these TLDs is malicious, understanding the general risk of the TLD itself can aid defenders in deciding whether there is a business case for blocking the TLD or, at the very least, in carefully monitoring it.

TLD	Months at high or very high risk
cam	6 / 6
cfd	6 / 6
click	6 / 6
quest	6 / 6
rest	6 / 6
ws	6 / 6
bid	5 / 6
icu	5 / 6
ml	5 / 6
top	5 / 6

Table 1: High-risk TLDs with the most consistently high confidence risk scores for the past two quarters.

While these are high-risk TLDs, they may still have legitimate domains that are well trafficked. The ten high-risk TLDs shown in Table 1 have a combined 85 domains in the Internet sites most popular according to Infoblox's InfoRanks (roughly equivalent to the top 3% of domains), which means that they can appear in our allowlists.

With the knowledge that some of these TLDs were both classified as high risk and have popular domains, researchers further analyzed the data to see what else they could learn. The first TLD of interest was the `top` TLD; while it didn't have the highest risk scores of all the TLDs, the sheer number of malicious domains observed warranted a deeper look. Figure 5 below shows the threat classifications of malicious domains for the past six months in the TLD `top`. Starting in June, there was a significant increase in the number of observed phishing and malware download domains. This peaked in July, which had a more than 500% increase over April in phishing domains alone.

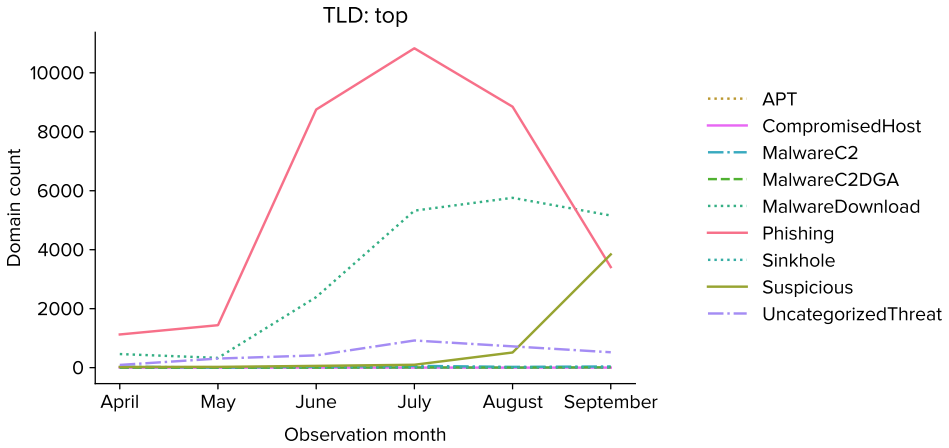


Figure 5: Totals for domains assigned to different threat classes in the TLD `top` for the past two quarters are shown. From May to July, the number of phishing domains increased by more than 500%.

Given the significant increase in the number of phishing domains, Infoblox researchers performed a more in-depth investigation into domains in the TLD `top`. Since January of 2022, over 30,000 domains were registered in the TLD that appear to have been generated using a dictionary domain generation algorithm (DDGA) similar to the VexTrio DDGA, previously reported by Infoblox researchers. In this case, the DDGA produced domain names that comprise two English words, resulting in domain names like `cardboardrefugee[.]top` and `momentumfrantically[.]top`. According to Infoblox analysis, over half of those domains are known to have been used for phishing at some point.

The TLD `quest` also saw a spike in phishing domains in June, as shown in Figure 6. However, it didn't see as much customer traffic as other TLDs, with slightly over 10% of customer traffic going to it. That doesn't mean it isn't a risky TLD, though. The phishing domains could have been part of a campaign targeting organizations such as those customers.

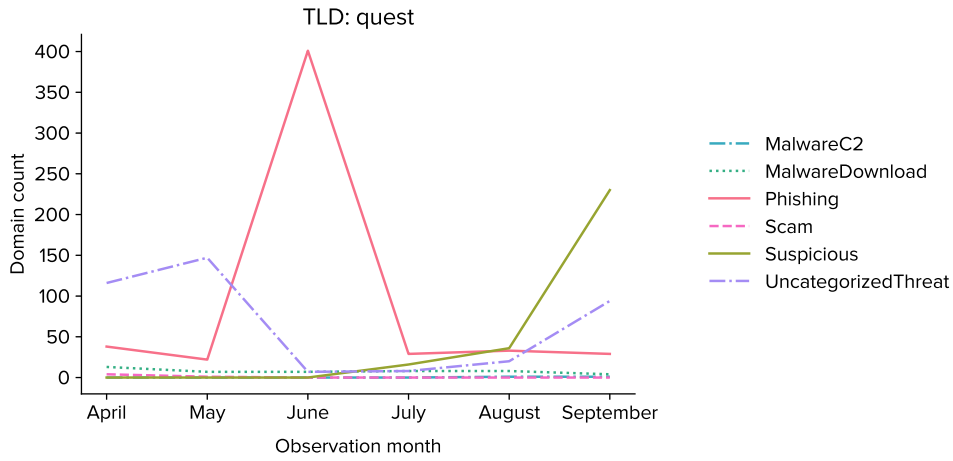
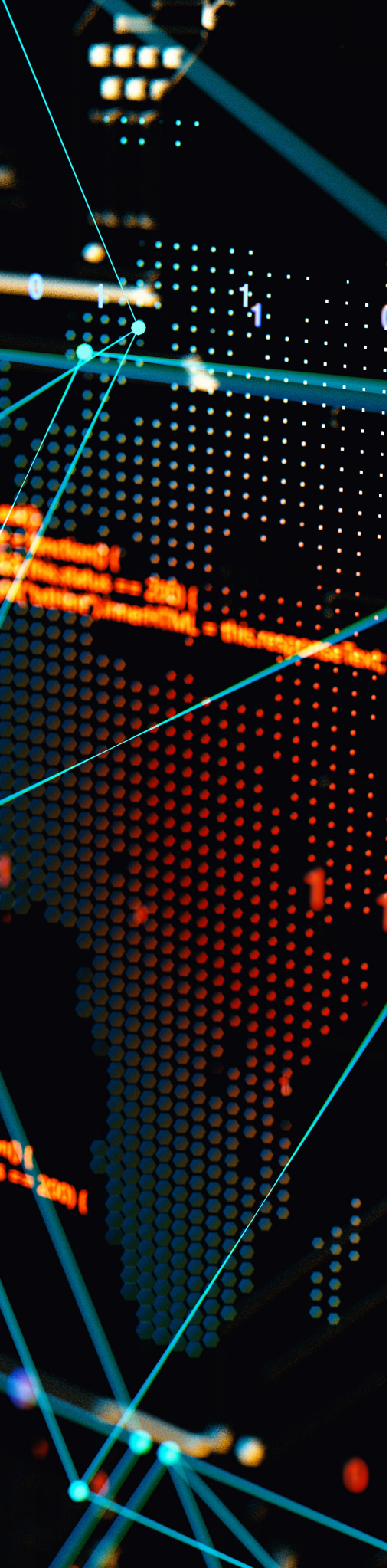


Figure 6: Totals for domains assigned to different threat classes in the TLD `quest` for the past two quarters.



Infoblox often receives threat intelligence from other organizations, such as government agencies, that lack details on the specific threat class, for understandable reasons. In these situations, Infoblox assigns the UncategorizedThreat threat class to the domain. Figure 7 illustrates an increase, peaking in June, in the numbers of these domains for the TLD `click`.

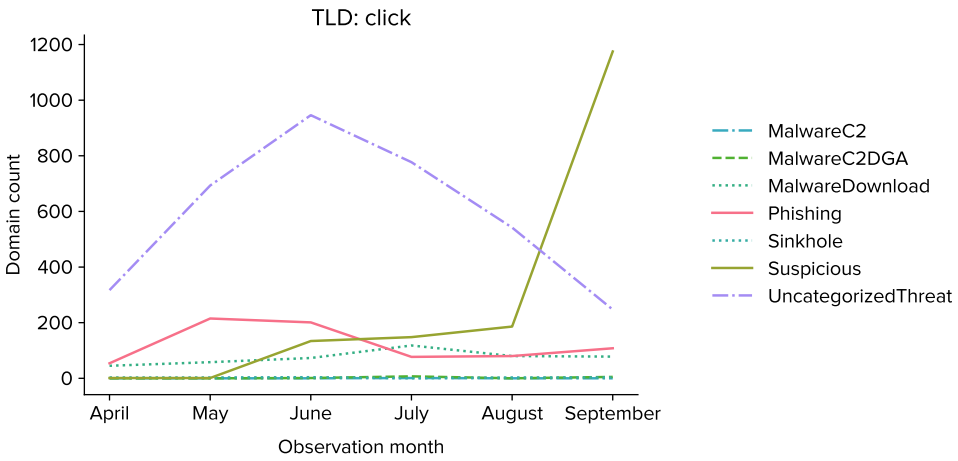


Figure 7: Totals for domains assigned to different threat classes in the TLD `click` for the past two quarters.

Future Directions

Infoblox's new reputation-scoring algorithm has already proven successful. Its application to determining TLD reputation has yielded information that Infoblox has used to strengthen the defenses of its customers through Dossier and other products. Future articles and quarterly reports will highlight its usefulness as researchers apply it to other data, such as nameservers and domain registrars, of which Infoblox has a unique view.

Emotet: A Malware Family That Keeps Going

Executive summary

Emotet is a notorious malware family that has evolved significantly over the years: from a simple banking trojan to a botnet to an infrastructure for content delivery. Infoblox has been monitoring Emotet and providing insights on its activity all along.

Emotet has been around since 2014. It survived its January 2021 takedown by law enforcement agencies from the Netherlands, UK, and US and from Germany, France, Lithuania, Canada, and Ukraine. During the takedown, Emotet was offline for 11 months.

The frequency of Emotet-related malspam campaigns increased from January to May 2022 as the malware authors changed techniques to evade Microsoft's increasing countermeasures on VBA Macro security. The Max Planck Institute for Plasma Physics was attacked on 12 June 2022, and recent reports put Emotet back at the top of the list of malware families with impact that spans the globe.[11] Infoblox has been monitoring the increase in Emotet activity, and our insights are captured in this report.

Emotet delivery vehicles

Since the 2021 takedown, a consistent feature of Emotet has been its use of email as a delivery vector. Microsoft Office documents have been the attachments of choice, and Excel files have been the most prevalent of these documents.

Since May 12, 2022, we have observed more than 60,000 malspam campaigns distributing 13,000 file hashes.

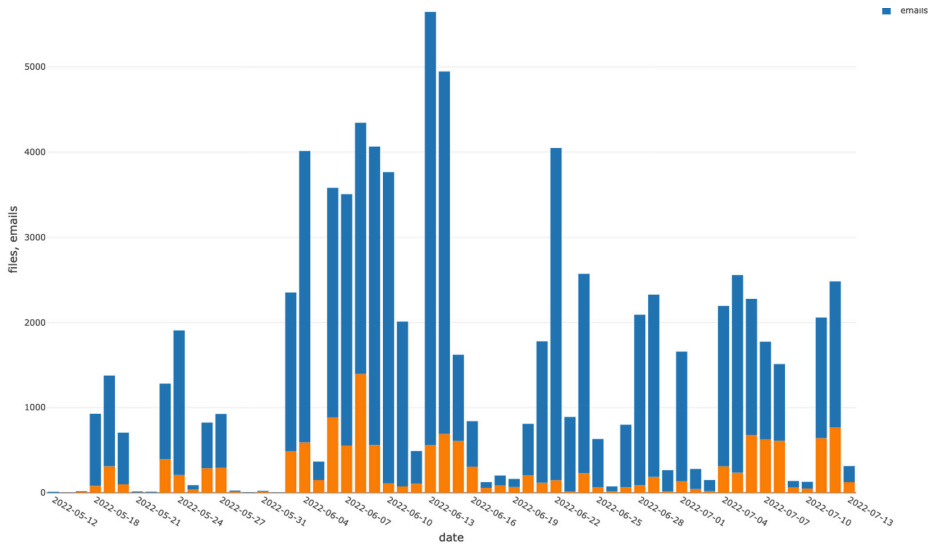


Figure 1: Distribution of Emotet's unique email IDs and file hashes from 12 May to 13 July 2022

The campaigns share some characteristics. In particular, they use "RE:", "FW:", and other well-known, tried-and-true generic lures in the subject lines. They also use generic shipping- and invoice-related keywords, presumably to make the messages appear legitimate. Some subject lines contain Ukraine-themed lures, which make the emails appear up-to-date with important events happening in the world. Figure 2 shows the subject lines and the most common themes used across the malspam campaigns spreading Emotet.

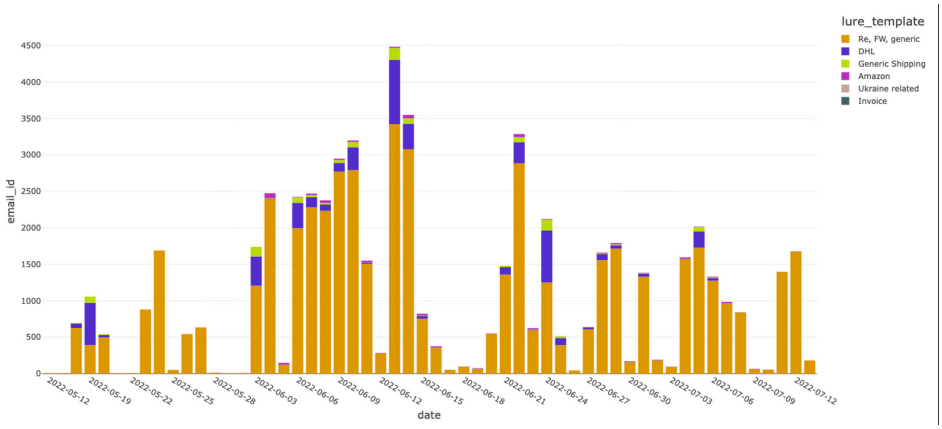


Figure 2: Distribution of subject lines across malspam email campaigns

Figure 2 illustrates that the primary non-generic lures used by Emotet aim to trick recipients into believing that the messages relate to Amazon or DHL deliveries. This technique has been used by attackers for several years and is not exclusive to Emotet. The next part of the analysis focuses on files attached to the emails.

File attachments analysis

The subject and body of an email that delivers Emotet are designed to trick a recipient into opening the attachment. Once opened, the attachment triggers malicious XLM macros and starts the chain of an Emotet infection.

Most email attachments contain a single Microsoft Excel file with XLM macros that include a link; clicking the link fetches the Emotet payload DLL. However, some attachments are zip archives. Figure 3 shows the distribution of all file types that Emotet used during our investigation. The graph clearly shows that Excel documents are most prevalent, followed by zip archives. In all cases where the attachment is a zip archive, the contents are an Excel document. One possible reason Microsoft Excel files are the preferred attachment type is that the corporate world moves slowly, and the patches or Microsoft updates are deployed very slowly, and this buys attackers additional time to infect the victims' computers. The attackers continue to use these infection techniques that capitalize on corporate users' tendencies to rely on outdated versions of Microsoft Office or to completely disable protection.

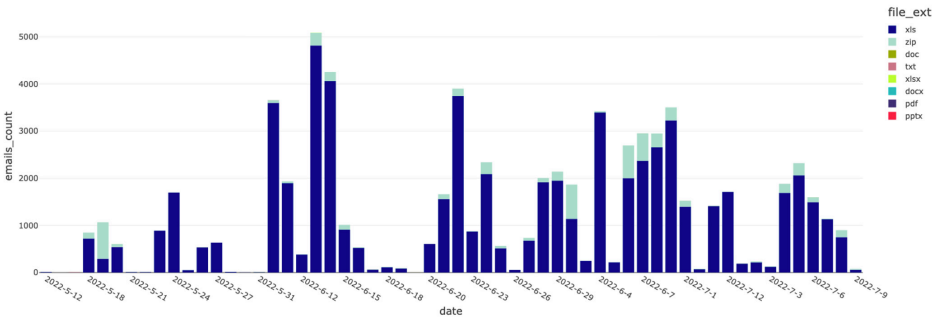


Figure 3: Distribution of Emotet-related emails per file type over time

The file attachments deploy well-known techniques for bypassing Windows protections and downloading the Emotet DLL file. In January 2022, in an effort to protect users against threats that leverage this technique, Microsoft released its latest advisory on disabling Excel XLM macros. However, because this will always remain a configurable feature, Infoblox continues to observe high volumes of malspam with macro-enabled attachments.

Malicious payloads domain distribution

To understand where the threat actors store the malicious DLL payloads, we analyzed approximately 13,000 attachments from Emotet emails; in addition, we extracted not only the URL pointing to the malicious Emotet DLL payload but also the hosting domains. We discovered that most of the domains being used to host the Emotet DLL payloads are compromised websites that are either poorly developed or badly maintained, and as such, provide a soft target for the attackers. To test this, we used Infoblox's patent-pending InfoRanks algorithms, which rank websites according to how frequently they are queried by Infoblox customers. In this case, the ranking indicates that the more popular or highly ranked a website is, the greater the likelihood is that the user is navigating to a legitimate but infected or compromised domain, rather than a domain owned by the threat actor.

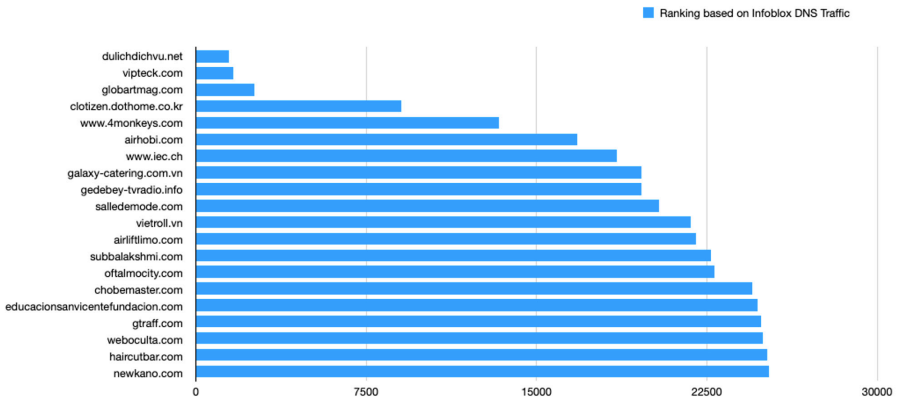


Figure 5: Most popular compromised websites (qnames) hosting or having hosted Emotet DLLs in the past four months, based on Infoblox customer traffic

Our research also highlights the importance of the longevity of a hosting domain. By evaluating the first and last times a domain is referenced in the Emotet email attachments, we can get a sense of the average period of time a compromised site is used by the Emotet actors.

Figure 6 shows the top 20 compromised domains. The score was determined from the number of compromised domains names extracted from Emotet-related file attachments.

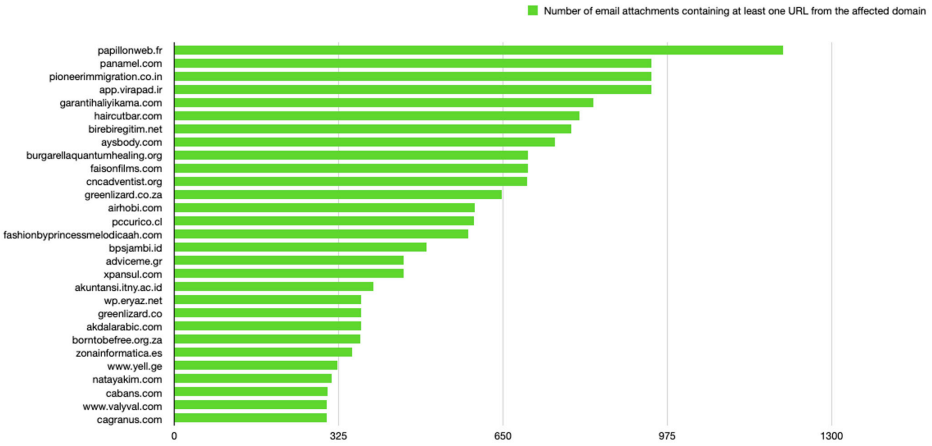


Figure 6: Top 20 compromised domains whose names were extracted from Emotet-related email file attachments

None of the top domains hosting the Emotet DLL payloads were newly registered. The following table displays some key statistics that can offer insights into why attackers consider compromised domains to be a preferable vector for distributing malware. The "Count of malicious file attachments" column shows the number of different files that used the same qname embedded in the XLMacro code for fetching the Emotet payload. The "Days used in Emotet campaigns" column shows the observed usage, in days, of the compromised domains. Essentially, this is the difference between the first and last days on which we spotted an Emotet-related Excel file with the specific qname embedded as part of the XLMacro code. Last but not least, the domain age is the number of days from the creation date of the specific SLD up to the day of our analysis.

qname	Count of malicious file attachments	Days used in Emotet campaigns	Domain age
papillonweb[.]fr	1204	26 days	3012 days
www[.]pioneerimmigration[.]co[.]in	944	10 days	682 days
panamel[.]com	944	10 days	5091 days
app[.]virapad[.]ir	943	2 days	-
www[.]garantihaliyikama[.]com	829	13 days	750 days
haircutbar[.]com	801	11 days	4570 days
www[.]birebiregitim[.]net	785	11 days	1453 days
aysbody[.]com	752	20 days	628 days
burgarellaquantumhealing[.]org	699	14 days	2056 days

faisonfilms[.]com	699	14 days	1509 days
cncadventist[.]org	698	14 days	2291 days
greenlizard[.]co[.]za	648	12 days	6677 days
airhobi[.]com	594	7 days	841 days
pccurico[.]cl	592	6 days	4356 days
fashionbyprincessmelodicaah[.]com	581	0 days	815 days
bpsjambi[.]id	498	36 days	413 days
xpansul[.]com	454	13 days	7590 days
adviceme[.]gr	454	13 days	-
akuntansi[.]itny[.]ac[.]id	393	6 days	1270 days
wp[.]eryaz[.]net	370	32 days	6951 days

Table 1: Most frequently used qnames in malspam file attachments downloading Emotet

Analysis of C&C infrastructure

After the Emotet DLL payload is executed, the command and control (C&C) communication is initiated. Emotet C&Cs consist of IP addresses accompanied by specific ports. Here, we analyze the C&C IPs to better understand the Emotet botnet and infrastructure. During the course of our analysis, we extracted and reviewed the C&C IPs from approximately 200 Emotet DLLs.

Emotet's global footprint

The C&C IP distribution is depicted on the world maps shown in Figures 7 and 8. We used data from the Feodo Tracker to compare the current Emotet C&Cs to the pre-takedown Emotet C&Cs. The map in Figure 7 shows the distribution of C&C IPs per country before the takedown. Comparison of the maps in Figures 7 and 8 reveals that Emotet C&Cs continue to be hosted primarily in the United States, but there is also a strong presence of Emotet in Europe. For example, the number of C&C server hosts has increased in Germany and France. The maps also show that the United States, Germany, France, India, and Indonesia are currently the countries of choice for hosting Emotet C&C infrastructure.

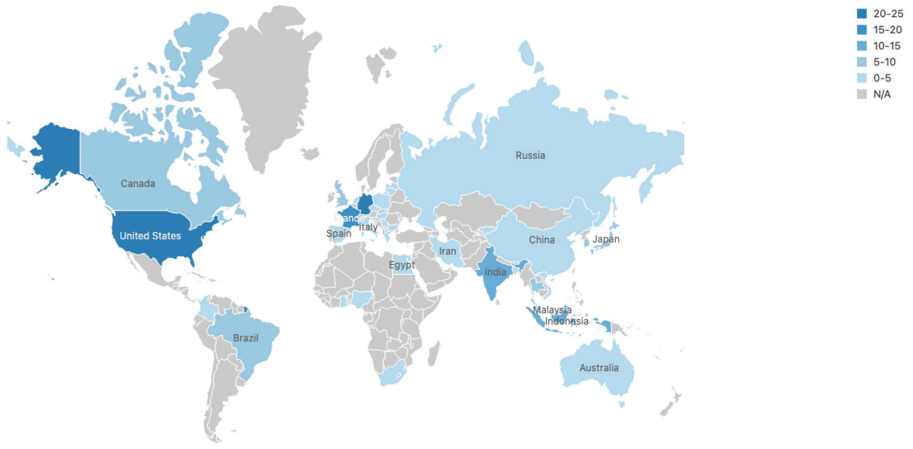


Figure 7: Post-takedown distribution of Emotet C&C servers

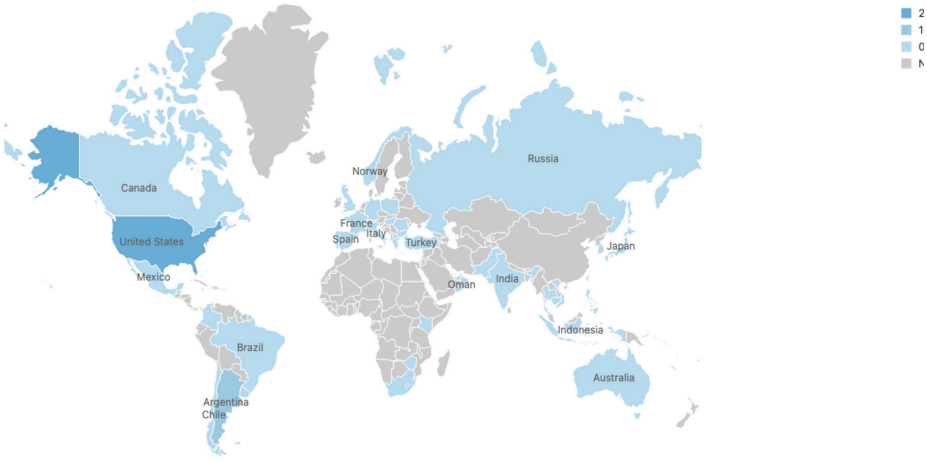


Figure 8: Pre-takedown distribution of Emotet C&C servers

Our analysis indicates that the C&C IPs are part of the virtual private cloud (VPC) infrastructure, which suggests that the current group operating Emotet chooses to pay for this service. In particular, we have observed that the use of Digital Ocean amongst other VPC providers has increased considerably. Before the takedown, most of the hosting providers used were telecommunications providers. Since the takedown, there has been an increase in the number of hosting providers that offer VPC solutions, which provide more privacy and make it more difficult for law enforcement agencies to conduct takedowns. Figures 9 and 10 show the significant shift from Telecom-related hosting infrastructure to cloud hosting infrastructure. Nevertheless, there is still 16% of the infrastructure hosted in telcos. Some company names that stand out are Korea Telecom, 1&1 AG, PT Telkom Indonesia and SK Broadband.

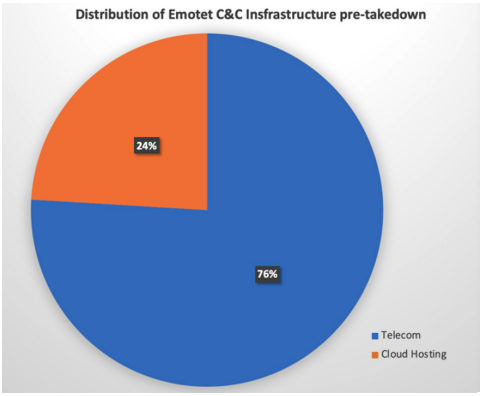


Figure 8: Pre-takedown distribution of Emotet C&C servers

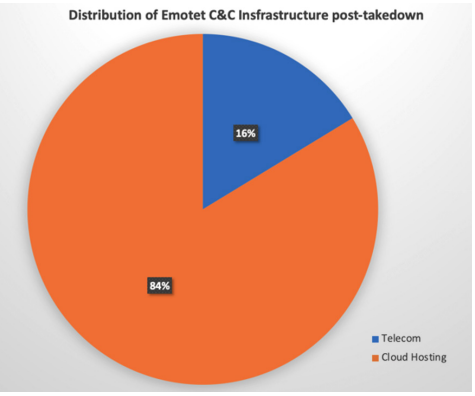


Figure 8: Post-takedown distribution of Emotet C&C servers

Prevention and mitigation

Despite its high-profile takedown in April 2021, Emotet remains active. In addition, our analysis indicates that the actors behind Emotet have made some attempts to protect the network from further takedowns. Perhaps unsurprisingly, the use of compromised websites and of email as a delivery vector has persisted, and this has enabled us to reliably identify and track Emotet's activity. Our view of the threat landscape affords a detailed understanding of not only the current prevalence of Emotet in malspam but also of the location and services used in its infrastructure.

As we continue to research and monitor Emotet's behavior, we will provide protection by denying access to the compromised domains used to host the Emotet payload, and we will offer vital, actionable intelligence on Emotet's C&C infrastructure.

We recommend the following actions for protection from this kind of an attack:

- To mitigate the risk of infection from known threats, keep security software up to date and patched.
- Conduct security awareness training in the organization. It is important for everyone to be up to date with the latest techniques used by attackers to trick users who receive malicious emails.
- Enhance network perimeter security. 99% of successful attacks involve some type of network communication. Having the right tools in place can help identify and minimize the impact of a threat like Emotet before they cause damage.

Indicators of compromise

The table below provides a sample list of the IOCs relevant to our recent findings. The complete list as of the time of this paper is found in our GitHub repository.

Indicator	Type
www[.]cicerosd[.]com	Emotet payload DLL download domain
chainandpyle[.]com	Emotet payload DLL download domain
www[.]visionsfantastic[.]com	Emotet payload DLL download domain

ent[.]draftserver[.]com	Emotet payload DLL download domain
www[.]evosp[.]com[.]br	Emotet payload DLL download domain
www[.]clinicaportalpsicologia[.]com[.]br	Emotet payload DLL download domain
greycoconut[.]com	Emotet payload DLL download domain
harleyqueretaro[.]com	Emotet payload DLL download domain
drviniciusterra[.]com[.]br	Emotet payload DLL download domain
dscaluya[.]6te[.]net	Emotet payload DLL download domain
www[.]concivilpa[.]com[.]py	Emotet payload DLL download domain
helmprecision[.]com	Emotet payload DLL download domain
www[.]megakonferans[.]com	Emotet payload DLL download domain
disperindag[.]garutkab[.]go[.]id	Emotet payload DLL download domain
www[.]ergbox[.]com	Emotet payload DLL download domain
blessingsource[.]com	Emotet payload DLL download domain
deadcode200[.]c1[.]biz	Emotet payload DLL download domain
cs14productions[.]com	Emotet payload DLL download domain
djunreal[.]co[.]uk	Emotet payload DLL download domain
fisika[.]mipa[.]uns[.]ac[.]id	Emotet payload DLL download domain
grouprobust[.]com	Emotet payload DLL download domain
jimlowry[.]com	Emotet payload DLL download domain
balticcontrolbd[.]com	Emotet payload DLL download domain
www[.]druck-grafik[.]at	Emotet payload DLL download domain
dl[.]choobingroup[.]ir	Emotet payload DLL download domain
www[.]dl5[.]zahra-media[.]ir	Emotet payload DLL download domain
astrogurusunilbarmola[.]com	Emotet payload DLL download domain
brittknight[.]com	Emotet payload DLL download domain
www[.]hayalkatibi[.]com	Emotet payload DLL download domain
wmwifbajxxbcxmucxmlc[.]com	Emotet payload DLL download domain

kevinley[.]com	Emotet payload DLL download domain
appyhorsey[.]com	Emotet payload DLL download domain
www[.]graduate[.]cmru[.]ac[.]th	Emotet payload DLL download domain
www[.]lakor[.]ch	Emotet payload DLL download domain
erp[.]pinaken[.]com	Emotet payload DLL download domain
corporateissolutions[.]com	Emotet payload DLL download domain
perpustekim[.]untirta[.]ac[.]id	Emotet payload DLL download domain
iciee[.]untirta[.]ac[.]id	Emotet payload DLL download domain
ikatemia[.]untirta[.]ac[.]id	Emotet payload DLL download domain
tm[.]gamester[.]com[.]tr	Emotet payload DLL download domain
dencker[.]info	Emotet payload DLL download domain
www[.]escueladecinemza[.]com[.]ar	Emotet payload DLL download domain
escueladecinemza[.]com[.]ar	Emotet payload DLL download domain
www[.]mobiles-photostudio[.]com	Emotet payload DLL download domain
iprd[.]net[.]phtemp[.]com	Emotet payload DLL download domain
charmslovespells[.]com	Emotet payload DLL download domain
ewingconsulting[.]com	Emotet payload DLL download domain
francite[.]net	Emotet payload DLL download domain
educacionsanvicentefundacion[.]com	Emotet payload DLL download domain
clotizen[.]dothome[.]co[.]kr	Emotet payload DLL download domain
gmhealthcare[.]dothome[.]co[.]kr	Emotet payload DLL download domain
kwinglobal[.]dothome[.]co[.]kr	Emotet payload DLL download domain
withvac001[.]dothome[.]co[.]kr	Emotet payload DLL download domain
onepieceark[.]dothome[.]co[.]kr	Emotet payload DLL download domain
www[.]zvdesign[.]info	Emotet payload DLL download domain
natdemo[.]natrixsoftware[.]com	Emotet payload DLL download domain
www[.]fcstradesolutions[.]com	Emotet payload DLL download domain
demo-re-usables[.]inertiasoft[.]net	Emotet payload DLL download domain
www[.]guedala[.]com[.]br	Emotet payload DLL download domain
www[.]berekethaber[.]com	Emotet payload DLL download domain

bruidsfotografie-breda[.]nl	Emotet payload DLL download domain
fontecmobile[.]com	Emotet payload DLL download domain
document[.]vpservice-online[.]com	Emotet payload DLL download domain
atperson[.]com	Emotet payload DLL download domain
frascona[.]com[.]ar	Emotet payload DLL download domain
cashmailsystem[.]com	Emotet payload DLL download domain
www[.]clasite[.]com	Emotet payload DLL download domain
kairaliagencies[.]com	Emotet payload DLL download domain
gedebey-tvradio[.]info	Emotet payload DLL download domain
decorusfinancial[.]com	Emotet payload DLL download domain
zachboyle[.]com	Emotet payload DLL download domain
www[.]boraintercambios[.]com[.]br	Emotet payload DLL download domain
peicovich[.]com	Emotet payload DLL download domain
www[.]federation-sardaniste[.]fr	Emotet payload DLL download domain
weboculta[.]com	Emotet payload DLL download domain
earthmach[.]co[.]za	Emotet payload DLL download domain
www[.]drcno[.]sk	Emotet payload DLL download domain
www[.]forensisbilisim[.]com	Emotet payload DLL download domain
www[.]fullwiz[.]com[.]br	Emotet payload DLL download domain
evashopping[.] thietkewebsitechuanseo[.]com	Emotet payload DLL download domain
travel[.]pkn2[.]go[.]th	Emotet payload DLL download domain
www[.]anglicanjoburg[.]org[.]za	Emotet payload DLL download domain
www[.]joburg[.]org[.]za	Emotet payload DLL download domain
mtc[.]joburg[.]org[.]za	Emotet payload DLL download domain
dotcompany[.]com[.]br	Emotet payload DLL download domain
comecebem[.]com	Emotet payload DLL download domain
collabsolutions[.]co[.]za	Emotet payload DLL download domain
borntobefree[.]org[.]za	Emotet payload DLL download domain

wp[.]eryaz[.]net	Emotet payload DLL download domain
akuntansi[.]itny[.]ac[.]id	Emotet payload DLL download domain
nycom[.]narasoft[.]com	Emotet payload DLL download domain
cupsolution[.]com	Emotet payload DLL download domain
wordpress[.]agrupem[.]com	Emotet payload DLL download domain
www[.]olsav[.]sk	Emotet payload DLL download domain
www[.]aseguradosaldia[.]com	Emotet payload DLL download domain
www[.]nomatenalmono[.]org	Emotet payload DLL download domain
www[.]diarioaldia[.]com[.]ar	Emotet payload DLL download domain
ftp[.]yuecmr[.]org	Emotet payload DLL download domain
contabilidadeplenus[.]com[.]br	Emotet payload DLL download domain
fashionbyprincessmelodicaah[.]com	Emotet payload DLL download domain
chaledooleo[.]com[.]br	Emotet payload DLL download domain
greenlizard[.]co[.]za	Emotet payload DLL download domain
nellydwiputri[.]co[.]id	Emotet payload DLL download domain
www[.]llev[.]com[.]br	Emotet payload DLL download domain
starluckycentre[.]com	Emotet payload DLL download domain
3dstudioa[.]com[.]br	Emotet payload DLL download domain
survei[.]absensi[.]net	Emotet payload DLL download domain
haircutbar[.]com	Emotet payload DLL download domain
www[.]garantihaliyikama[.]com	Emotet payload DLL download domain
dusangerzicgera[.]com	Emotet payload DLL download domain
ybp[.]rpmediateam[.]com	Emotet payload DLL download domain
www[.]controlnetworks[.]com[.]au	Emotet payload DLL download domain
app[.]virapad[.]ir	Emotet payload DLL download domain
54[.]37[.]106[.]167	Emotet C&C IP
78[.]47[.]204[.]80	Emotet C&C IP
202[.]28[.]34[.]99	Emotet C&C IP
210[.]57[.]209[.]142	Emotet C&C IP
118[.]98[.]72[.]86	Emotet C&C IP

37[.]44[.]244[.]177	Emotet C&C IP
196[.]44[.]98[.]190	Emotet C&C IP
195[.]77[.]239[.]39	Emotet C&C IP
139[.]196[.]72[.]155	Emotet C&C IP
54[.]37[.]228[.]122	Emotet C&C IP
62[.]171[.]178[.]147	Emotet C&C IP
202[.]134[.]4[.]210	Emotet C&C IP
85[.]214[.]67[.]203	Emotet C&C IP
93[.]104[.]209[.]107	Emotet C&C IP
88[.]217[.]172[.]165	Emotet C&C IP
103[.]41[.]204[.]169	Emotet C&C IP
87[.]106[.]97[.]83	Emotet C&C IP
85[.]25[.]120[.]45	Emotet C&C IP
202[.]29[.]239[.]162	Emotet C&C IP
36[.]67[.]23[.]59	Emotet C&C IP
175[.]126[.]176[.]79	Emotet C&C IP
103[.]56[.]149[.]105	Emotet C&C IP
178[.]62[.]112[.]199	Emotet C&C IP
104[.]248[.]225[.]227	Emotet C&C IP
188[.]225[.]32[.]231	Emotet C&C IP
103[.]85[.]95[.]4	Emotet C&C IP
104[.]244[.]79[.]94	Emotet C&C IP
157[.]230[.]99[.]206	Emotet C&C IP
103[.]126[.]216[.]86	Emotet C&C IP
157[.]245[.]111[.]0	Emotet C&C IP

Omnatuor Malvertising Network Hijacks Browser Settings to Spread Riskware

Summary

For some time, the Infoblox Threat Intelligence Group has been tracking a malvertising network (the "Omnatuor Malvertising Network") that not only abuses push notifications, pop-ups, and redirects within a browser but continues to serve ads even after the user navigates away from the initial page. Omnatuor has been dismissed by the security community as adware, a label that implies the activity is largely a nuisance. This naive response underestimates the danger of the potential threat posed by malvertising in general, and the Omnatuor actor in particular. In addition to its ability to persist, the network delivers dangerous content.

Infobox has discovered and begun tracking multiple malvertising networks with a very broad reach into the consumer environment. They obtain this reach by locating and compromising massive numbers of web pages across the Internet and then relying on the tendency of users to click the accept buttons on pop-ups without carefully examining the notifications. We recently published an in-depth report about one of these actors and their network we call VexTrio.

The Omnatuor actor, like the VexTrio actor, takes advantage of WordPress vulnerabilities and is effective at spreading riskware, spyware, and adware. Also like the VexTrio actor, the Omnatuor actor uses an extensive infrastructure and has a broad reach into networks across the globe. We found over 9,900 domains and 170 IP addresses related to the original "seed" domain, omnatuor[.]com. Unlike the VexTrio actor, the Omnatuor actor uses a clever technique to achieve persistence across a user's browsing patterns.

This report will provide detailed information about the actor's techniques, tactics, and procedures (TTP). We detail the infrastructure, scope of activity, attack chain, preventative measures and remediation and, finally, indicators of compromise (IOCs). We have included a sample of these IOCs at the end of this report; for the complete list, see our GitHub repository. Watch this podcast episode of ThreatTalk to learn more about the Omnatuor network, phishing and malvertising.

Discovery

Our research into the Omnatuor Malvertising Network began with the discovery of an initial domain, omnatuor[.]com. The prevalence of this domain and the number of queries across many networks raised our attention. Highly popular domains are usually related to common applications and services (such as Outlook and Google), content distribution networks, and ad networks. The Omnatuor domain has suspiciously high breadth and query volumes. An initial look into WHOIS data revealed the domain was created on 12 July 2021. Since being registered it was present in 45% to 48% of all customer networks and surpassed 50% at various times, as shown in Figure 1.

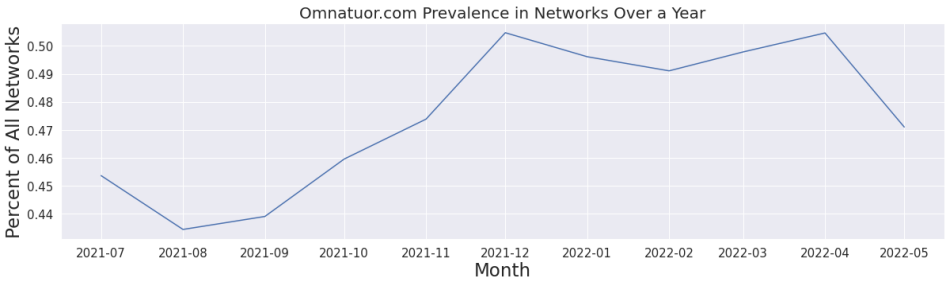


Figure 1. Omnatuor[.]com saturation across Infoblox networks following registration in July 2021.

Most networks contained tens, if not hundreds, of thousands of queries for the domain. From July 2021 to July 2022, we observed just over 25.4 million unique, resolved queries to omnatuor[.]com. To discover new domains related to omnatuor[.]com, we used passive DNS (pDNS) data; leveraged open-source forum posts involving at least one previously discovered domain or IP address; checked domain, file, and IP relationships by using URLScan (urlscan[.]io), VirusTotal (virustotal[.]com), and other open-source tools; and used virtual machines to explore websites that we knew to be infected with an adware script. In the course of our research, we found over 9,900 domains and 170 IP addresses comprising the Omnatuor Malvertising Network.

We utilized our previous research on domain-ranking systems and our internal ranking system, InfoRanks, to gain further perspective on the impact of not just omnatuor[.]com but the full Omnatuor Malvertising Network. We wanted to see just how popular the domains within this network had become in comparison to well-known websites. We took a random sample of nearly 700 domains from the pool of 9,900 and averaged their ranking in our aggregate data over 5 months. We then took all the malvertising domains in our sample and plotted them amongst other popular domains (whose popularity is based on InfoRanks). Figure 2 illustrates that in terms of the query count, the malvertising domains' relative popularity (in red) rivaled that of other well-known websites ranked within the top 10,000 most popular domains.

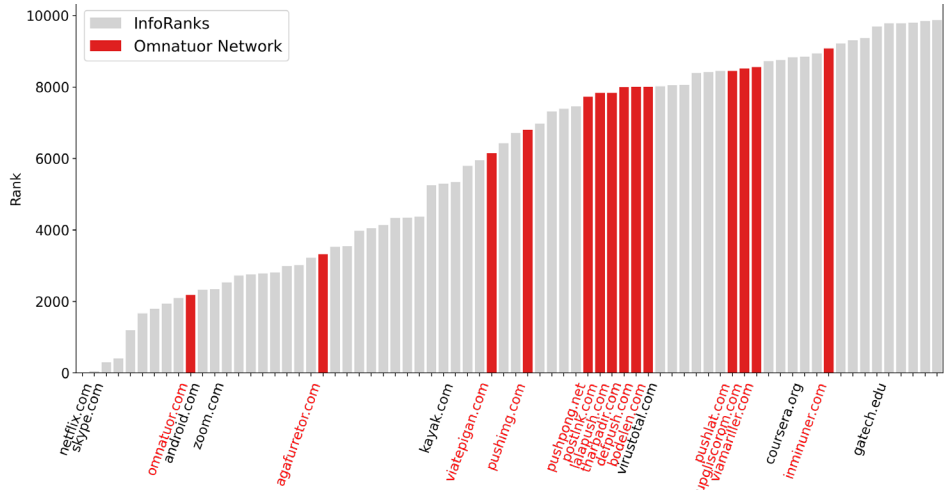


Figure 2. Omnatuor Malvertising Network domains ranked relative to other popular (measured via InfoRanks) domains.

We designate any domain with an average ranking of 20,000 or less as quite popular, and any domain with an average ranking of 5,000 or less as very popular. According to our analysis, omnatuor[.]com was not only in the top 2,000 most popular domains but ranked higher than zoom[.]com over a period of five months. This is due to the prevalence of the actor's infrastructure and the actor's use of resolutions with a time-to-live value of zero seconds, which helps avoid the DNS cache.

Infrastructure

Several key factors related to the domains helped uncover the infrastructure. First, most of the domains were on one of two IP networks: 139.45.0.0/16 and 188.42.0.0/16. At this time, the Autonomous System Numbers (ASNs) for the networks are 9002 and 35415, respectively. ASN 35415 was present in two open-source lists of bad ASNs. RETN, Limited provided the infrastructure for the 139.45.0.0/16 network, and WebZilla provided the infrastructure for the 188.42.0.0/16 network. A Cyprus-based "adtech" company owns the IP space that hosts the domains at the time of this report. A number of domains were hosted on one network before being switched to the other.

Second, all domains used the same registrar, Pananames (formerly URL Solutions, Inc.), which is located in Panama and offers low-cost domain registration. Furthermore, each domain in the Omnatuor Malvertising Network utilized Pananames' WHOIS privacy services, greatly limiting the visibility into the actor. Pananames, like the owner of the IP space on which the Omnatuor Malvertising Network is hosted, has ties to Cyprus.

Third, the vast majority of domains used Amazon Web Services nameservers (the actor used Amazon Route 53), and fewer than 20 domains were parked at bodis[.]com. Each domain had a set of four different nameservers with the following structure (below, we use the regular expression syntax "[0-9]+", which can be read as "one or more digits"):

ns-[0-9]+.awsdns-[0-9]+.com
ns-[0-9]+.awsdns-[0-9]+.net
ns-[0-9]+.awsdns-[0-9]+.org
Ns-[0-9]+.awsdns-[0-9]+.co.uk

There was little repetition of nameservers across domains; one sample of 1,000 domains contained 1,716 different nameservers. The most often shared nameserver was ns-691[.]awsdns-22[.]net, and it had a count of nine.

Attack Chain

Figure 3 below shows the attack chain for domains in the Omnatuor Malvertising Network, which is similar to what we observed during our research and monitoring of threat activity centered around a dictionary domain generation algorithm (DDGA) actor we named VexTrio, which likewise distributes riskware, spyware, and adware. We use language from the MITRE ATT&CK Framework to describe the attack chain.

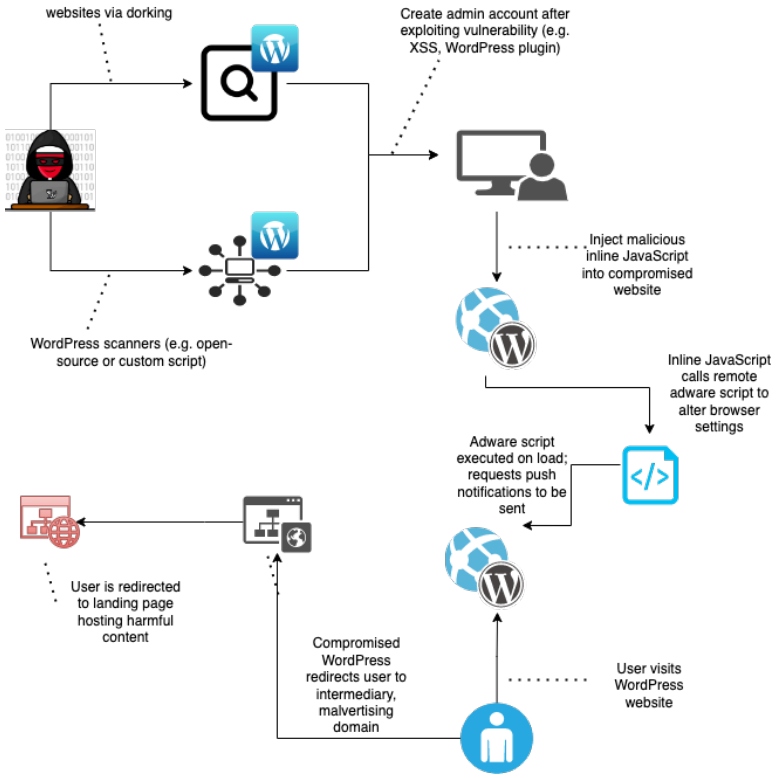


Figure 3. The Omnatuor attack chain.

Attack Chain: Initial Access

In our research, we initially found a handful of web page titles, such as *Remove Omnatuor.com pop-up ads (Virus Removal Guide)* and posts on the Malwarebytes forum where users were complaining of incessant advertisements and of struggling to identify where their browsers were first infected. In spite of the prolific number of sites offering advice on how to remove the adware, we found no reporting in the security industry that recognizes either the threat posed by this network or the depth and breadth of its penetration.

Older reports for similar attacks published by security vendors suggested that a cross-site scripting attack conducted via WordPress-specific malicious plugins (packaged as JavaScript or PHP code) might be the initial vector for contaminating sites. In such a case, the actors scan WordPress sites for vulnerabilities by using well-documented open-source software or Google dorking. Once the actors identify vulnerable sites, they inject into the body of the HTML an inline script that loads the adware remotely. We hypothesized that this might be the initial vector, too.

To test our hypothesis, we did our own Google dorking and verified that cross-site scripting attacks were the initial vector. We found a number of WordPress sites containing similar inline scripts. These inline scripts contained domains previously known to us as being part of the Omnatuor Malvertising Network. Figure 4 below shows source code from a compromised WordPress website, including the injected script (inside the red box) with context (arrows pointing to WordPress artifacts).

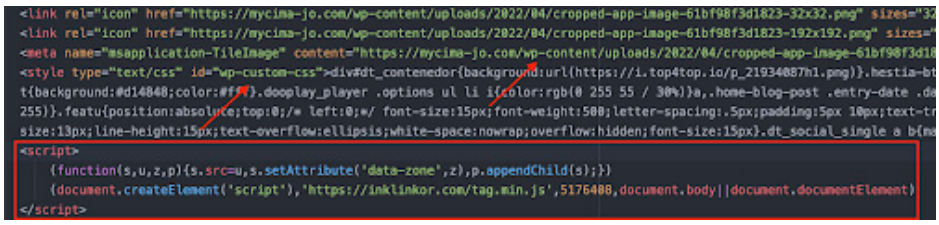


Figure 4. The compromise embedded in a victimized website's source code.

Attack Chain: Execution

Once a site is compromised, the adware script is executed upon page load. The entirety of the adware script – including names of variables, functions and domains, and even whole strings – is obfuscated. The obfuscation process is involved, but as with all source code obfuscation, the weakest link is the encryption. In this case, the actors used poor technique. We saw actors use two versions of a Caesar cipher, which shifts the alphabet a certain number of characters. One version shifted letters by 12 characters, and the other shifted letters by 13.

On page load, a function performs two steps to turn the code into runnable JavaScript:

1. It checks for a single character or for double characters in an array and returns a string obfuscated via the Caesar cipher.

2. It decrypts the obfuscated string into a machine-interpretable variable or value.

After the adware script is loaded, the webpage begins to make callbacks to malvertising domains. Figure 5 contains a WireShark screenshot exemplifying the network connections to the malicious IP range after the adware script has been executed upon page load:

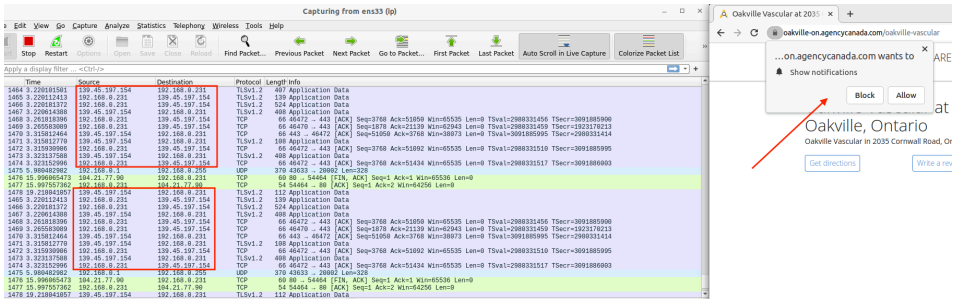


Figure 5. Network communication with the aforementioned malvertising C&C IP network.

The malvertising domains pass to the localhost JSON files containing redirect URLs, IDs for the ads, banners, trackers, and other information needed for the ad campaign. In a unique case, alongside two other Omnatuor-related malvertising domains, there was a JSON response containing a hardcoded BitRAT C&C IP shown in Figure 6.

BitRAT, as the name implies, is a remote access trojan (RAT). It originally surfaced in 2020 as an inexpensive, yet powerful, RAT that not only supports "generic keylogging, clipboard monitoring, webcam access, audio recording, credential theft from web browsers, and XMRig coin mining functionality" but also has the potential to bypass user access control. Whether there is a direct link between the spread of BitRAT and these malvertising domains is unclear, but the fact that a BitRAT C&C IP is sent back to the localhost from a malvertising domain suggests that it poses a notable risk.


```
{
    "status": true,
    "code": "jsTagParameters",
    "message": "",
    "unsupported": false,
    "afterCloseDelay": 3,
    "allowPopupIfHttpsDenied": true,
    "customParamsGeo": "de",
    "customParamsIp": "185.213.155.164",
    "domain": "https://jouteetu.net",
    "injections": null,
    "install_ctx": {
        "country_code": "de"
    },
    "resources": {},
    "mobileSupport": true,
    "popupHeight": 310,
    "popupShow": true,
    "popupWidth": 510,
    "pubZoneId": 5176469,
    "key": {
        "id": 780874806,
        "key": "BNMa9L2cERXXtndHqdfFHF5pjCBnZ_fic8IscI3ekLhWpAbHpKHhjW9MDGClSlpWzwgQMFVuS3tAGuIBR8aSr-c"
    },
    "swName": "sw.js",
    "wildcardDomain": "boustahe.com",
    "zoneId": 5176469,
    "skinUrl": "/pfe/current/defaultSkin.min.js",
    "popupUrl": "/pfe/current/popup.html",
    "flags": {},
    "extra": null
}
```


Figure 6. JSON response containing a BitRat IP address, denoted as "customParamsIp".

Attack Chain: Persistence

To maintain persistence, the actors must alter browser settings; to achieve this, they request the user to enable push notifications. If the user accepts the request, the actors modify the browser settings to allow the malvertising domains to send advertisements even after the user closes the browser window or goes to another site. Figure 7 shows an example of a push notification request.

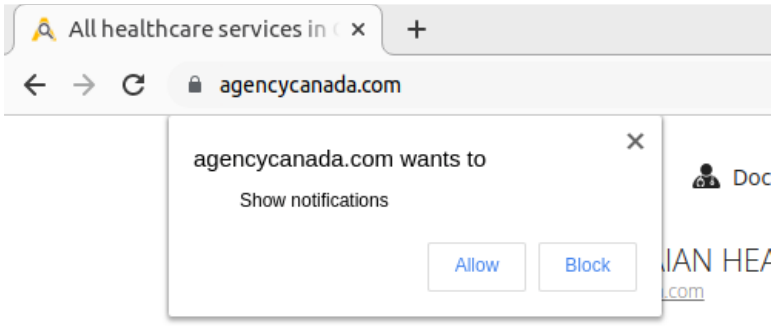


Figure 7. A malicious push notification request.

Recommendations and Mitigation

This campaign compromises vulnerable WordPress sites through embedded malicious JavaScript or PHP code. The code redirects users or otherwise forces them to view and click malvertisements via pop-ups and push notifications. We recommend that users take the following preventive measures:

- Configure Infoblox's RPZ feeds in DNS firewalls. This can stop the actors' attempts to connect at the DNS level, because all components described in this report (compromised websites, intermediary redirect domains, DDGA domains, and landing pages) require the DNS protocol. TIG detects these components daily and adds them to Infoblox's RPZ feeds.
- To assist in blocking known malvertising efforts, leverage the GitHub repository of indicators associated with the Omnatuor Malvertising Network.[32] Infoblox offers a sample of indicators in this article and will continue to update the GitHub repository as new indicators are discovered.
- Use an adblocker program, such as UBlock Origin. The adware is delivered via an inline script, and blocking only the domains and IP addresses at a firewall or DNS level will not stop push notifications, redirects, or pop-ups. Because the DNS query cannot be completed, the contents of those vectors will not load; however, the browsing experience will still be interrupted.
- Disable JavaScript entirely, or use a web extension (such as NoScript) to enable JavaScript only on trusted sites.

Indicators of Compromise

The table below provides a sample list of the IOCs relevant to our recent findings. The complete list as of the time of this paper is found in our GitHub repository.

Indicator	Description
139[.]45[.]197[.]148 139[.]45[.]197[.]247 139[.]45[.]197[.]235 139[.]45[.]197[.]234 139[.]45[.]197[.]187 139[.]45[.]197[.]186 139[.]45[.]197[.]157 139[.]45[.]197[.]148 139[.]45[.]197[.]253 139[.]45[.]197[.]152 185[.]213[.]155[.]164 188[.]42[.]224[.]59 188[.]42[.]224[.]60 188[.]42[.]224[.]61 188[.]42[.]224[.]62	Sample IP Addresses hosting the Omnatuor Malvertising Network Domains

omnatuor[.]com choogeet[.]net eeksoabo[.]com ptidsezi[.]com uthounie[.]com ugyplysh[.]com agafurretor[.]com omphantumpom[.]com sendmepush[.]com sbscribeme[.]com pushanishe[.]com pblcpush[.]com publpush[.]com pushno[.]com pushlommy[.]com pushlat[.]com pushlaram[.]com pushazer[.]com pushame[.]com pushails[.]com ptoafauz[.]net ptauxofi[.]net inpage-push[.]net propu[.]sh aaudrowqxuaws[.]xyz vjnccncigyiapw[.]xyz qnnmyjnnaoohdv[.]xyz	Sample of Omnatuor Malvertising Network Domains

CISA Alerts: Q3 2022

The Cybersecurity and Infrastructure Security Agency (CISA) is a U.S. government agency which leads a national effort to understand, manage, and reduce risk to both cyber and physical infrastructure. CISA connects stakeholders in industry and government to resources, analysis, and tools to help them design and build resilient and secure cyber, communications, and physical security.

Official CISA updates help stakeholders guard against the evolving ransomware threat environment. These alerts, current activity reports, analysis reports, and joint statements are geared toward system administrators and other technical staff to bolster their organization's security posture. These alerts provide timely information about current security issues, vulnerabilities, and exploits. More information on CISA alerts can be found here: https://www.cisa.gov/uscert/ncas/alerts.

AA22-265A: Control System Defense: Know the Opponent

Traditional approaches to securing OT/ICS do not adequately address current threats. Operational technology/industrial control system (OT/ICS) assets that operate, control, and monitor day-to-day critical infrastructure and industrial processes continue to be an attractive target for malicious cyber actors. These cyber actors, including advanced persistent threat (APT) groups, target OT/ICS assets to achieve political gains, economic advantages, or destructive effects. Because OT/ICS systems manage physical operational processes, cyber actors' operations could result in physical consequences, including loss of life, property damage, and disruption of National Critical Functions.

OT/ICS devices and designs are publicly available, often incorporate vulnerable information technology (IT) components, and include external connections and remote access that increase their attack surfaces. In addition, a multitude of tools are readily available to exploit IT and OT systems. As a result of these factors, malicious cyber actors present an increasing risk to ICS networks.

Traditional approaches to securing OT/ICS do not adequately address current threats to those systems. However, owners and operators who understand cyber actors' tactics, techniques, and procedures (TTPs) can use that knowledge when prioritizing hardening actions for OT/ICS. This joint Cybersecurity Advisory, which builds on previous NSA and CISA guidance to stop malicious ICS activity and reduce OT exposure, describes TTPs that malicious actors use to compromise OT/ICS assets. It also recommends mitigations that owners and operators can use to defend their systems. NSA and CISA encourage OT/ICS owners and operators to apply the recommendations in this CSA.

Download the PDF version of this report: pdf, 538.12 kb

AA22-264A : Iranian State Actors Conduct Cyber Operations Against the Government of Albania

The FBI and the Cybersecurity and Infrastructure Security Agency are releasing this joint Cybersecurity Advisory to provide information on recent cyber operations against the Government of Albania in July and September. This advisory provides a timeline of activity observed, from initial access to execution of encryption and wiper attacks.

In July 2022, Iranian state cyber actors—identifying as "HomeLand Justice"—launched a destructive cyber attack against the Government of Albania which rendered websites and services unavailable. A FBI investigation indicates Iranian state cyber actors acquired initial access to the victim's network approximately 14 months before launching the destructive cyber attack, which included a ransomware-style file encryptor and disk wiping malware. The actors maintained continuous network access for approximately a year, periodically accessing and exfiltrating e-mail content.

Between May and June 2022, Iranian state cyber actors conducted lateral movements, network reconnaissance, and credential harvesting from Albanian government networks. In July 2022, the actors launched ransomware on the networks, leaving an anti-Mujahideen E-Khalq (MEK) message on desktops. When

network defenders identified and began to respond to the ransomware activity, the cyber actors deployed a version of ZeroCleare destructive malware.

In June 2022, HomeLand Justice created a website and multiple social media profiles posting anti-MEK messages. On July 18, 2022, HomeLand Justice claimed credit for the cyber attack on Albanian government infrastructure. On July 23, 2022, Homeland Justice posted videos of the cyber attack on their website. From late July to mid-August 2022, social media accounts associated with HomeLand Justice demonstrated a repeated pattern of advertising Albanian Government information for release, posting a poll asking respondents to select the government information to be released by HomeLand Justice, and then releasing that information—either in a .zip file or a video of a screen recording with the documents shown.

In September 2022, Iranian cyber actors launched another wave of cyber attacks against the Government of Albania, using similar TTPs and malware as the cyber attacks in July. These were likely done in retaliation for public attribution of the cyber attacks in July and severed diplomatic ties between Albania and Iran.

Download the PDF version of this report: pdf, 1221 kb
Download the STIX file: pdf, 44 KB

AA22-257A : Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations

This joint Cybersecurity Advisory (CSA) is the result of an analytic effort among the FBI, the CISA, the National Security Agency (NSA), U.S. Cyber Command (USCC) - Cyber National Mission Force (CNMF), the Department of the Treasury (Treasury), the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), and the United Kingdom's National Cyber Security Centre (NCSC) to highlight continued malicious cyber activity by APT actors that the authoring agencies assess are affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC). Note: The IRGC is an Iranian Government agency tasked with defending the Iranian Regime from perceived internal and external threats. Hereafter, this advisory refers to all the coauthors of this advisory as "the authoring agencies."

This advisory updates joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities, which provides information on these Iranian government-sponsored APT actors exploiting known Fortinet and Microsoft Exchange vulnerabilities to gain initial access to a broad range of targeted entities in furtherance of malicious activities, including ransom operations. The authoring agencies now judge these actors are an APT group affiliated with the IRGC.

Since the initial reporting of this activity in the FBI Liaison Alert System (FLASH) report APT Actors Exploiting Fortinet Vulnerabilities to Gain Access for Malicious Activity from May 2021, the authoring agencies have continued to observe these IRGC-affiliated actors exploiting known vulnerabilities for initial access. In addition to exploiting Fortinet and Microsoft Exchange vulnerabilities, the authoring agencies have observed these APT actors exploiting VMware Horizon Log4j vulnerabilities for initial access. The IRGC-affiliated actors have used this access for follow-on activity, including disk encryption and data extortion, to support ransom operations.

The IRGC-affiliated actors are actively targeting a broad range of entities, including entities across multiple U.S. critical infrastructure sectors as well as Australian, Canadian, and United Kingdom organizations. These actors often operate under the auspices of Najee Technology Hooshmand Fater LLC, based in Karaj, Iran, and Afkar System Yazd Company, based in Yazd, Iran. The authoring agencies assess the actors are exploiting known vulnerabilities on unprotected networks rather than targeting specific targeted entities or sectors.

This advisory provides observed tactics, techniques, and IOCs that the authoring agencies assess are likely associated with this IRGC-affiliated APT.

For a downloadable copy of IOCs, see AA22-257A.stix.

For more information on Iranian state-sponsored malicious cyber activity, see CISA's Iran Cyber Threat Overview and Advisories webpage and FBI's Iran Threat webpage.

Download the PDF version of this report: pdf, 836 kb

AA22-249A : #StopRansomware: Vice Society

Note: This joint CSA is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed TTPs and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

The FBI, the CISA, and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint CSA to disseminate IOCs and TTPs associated with Vice Society actors identified through FBI investigations as recently as September 2022. The FBI, CISA, and the MS-ISAC have recently observed Vice Society actors disproportionately targeting the education sector with ransomware attacks.

Over the past several years, the education sector, especially kindergarten through twelfth grade (K-12) institutions, have been a frequent target of ransomware attacks. Impacts from these attacks have ranged from restricted access to networks and data, delayed exams, canceled school days, and unauthorized access to and theft of personal information regarding students and staff. The FBI, CISA, and the MS-ISAC anticipate attacks may increase as the 2022/2023 school year begins and criminal ransomware groups perceive opportunities for successful attacks. School districts with limited cybersecurity capabilities and constrained resources are often the most vulnerable; however, the opportunistic targeting often seen with cyber criminals can still put school districts with robust cybersecurity programs at risk. K-12 institutions may be seen as particularly lucrative targets due to the amount of sensitive student data accessible through school systems or their managed service providers.

The FBI, CISA, and the MS-ISAC encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

Download the PDF version of this report: pdf, 521 KB
Download the IOCs: .stix 31 kb

AA22-228A : Threat Actors Exploiting Multiple CVEs Against Zimbra Collaboration Suite

The CISA and the Multi-State Information Sharing & Analysis Center (MS-ISAC) are publishing this joint Cybersecurity Advisory (CSA) in response to active exploitation of multiple Common Vulnerabilities and Exposures (CVEs) against Zimbra Collaboration Suite (ZCS), an enterprise cloud-hosted collaboration software and email platform. CVEs currently being exploited against ZCS include:

- CVE-2022-24682
- CVE-2022-27924
- CVE-2022-27925 chained with CVE-2022-37042
- CVE-2022-30333

Cyber threat actors may be targeting unpatched ZCS instances in both government and private sector networks. CISA and the MS-ISAC strongly urge users and administrators to apply the guidance in the Recommendations section of this CSA to help secure their organization's systems against malicious cyber activity. CISA and the MS-ISAC encourage organizations who did not immediately update their ZCS instances upon patch release, or whose ZCS instances were exposed to the internet, to assume compromise and hunt for malicious activity using the third-party detection signatures in the Detection Methods section of this CSA. Organizations that detect potential compromise should apply the steps in the Incident Response section of this CSA.

Update September 27, 2022:

This CSA has been updated with additional IOCs. For a downloadable copy of the IOCs, see the following Malware Analysis Reports (MARs):

- MAR-10400779-1
- MAR-10400779-2
- MAR-10401765-1

Update End

Download the PDF version of this report: pdf, 427 kb
Download the IOCs: .stix 14 kb

AA22-223A : #StopRansomware: Zeppelin Ransomware

Note: this joint CSA is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed TTPs and IOCs to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

The FBI and the CISA are releasing this joint CSA to disseminate known Zeppelin ransomware IOCs and TTPs associated with ransomware variants identified through FBI investigations as recently as 21 June 2022.

The FBI and CISA encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

Download the PDF version of this report: pdf, 999 kb
Download the YARA signature for Zeppelin: YARA Signature, .yar 125 kb
Download the IOCs: .stix 113 kb

AA22-216A : 2021 Top Malware Strains

This joint CSA was coauthored by the CISA and the ACSC.This advisory provides details on the top malware strains observed in 2021. Malware, short for "malicious software," can compromise a system by performing an unauthorized function or process. Malicious cyber actors often use malware to covertly compromise and then gain access to a computer or mobile device. Some examples of malware include viruses, worms, trojans, ransomware, spyware, and rootkits.

In 2021, the top malware strains included remote access Trojans (RATs), banking Trojans, information stealers, and ransomware. Most of the top malware strains have been in use for more than five years with their respective code bases evolving into multiple variations. The most prolific malware users are cyber criminals, who use malware to deliver ransomware or facilitate theft of personal and financial information.

CISA and ACSC encourage organizations to apply the recommendations in the Mitigations sections of this joint CSA. These mitigations include applying timely patches to systems, implementing user training, securing Remote Desktop Protocol (RDP), patching all systems especially for known exploited vulnerabilities, making offline backups of data, and enforcing multifactor authentication (MFA).

Download the PDF version of this report: pdf, 576 kb

AA22-187A : North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector

The FBI, CISA, and the Department of the Treasury (Treasury) are releasing this joint CSA to provide information on Maui ransomware, which has been used by North Korean state-sponsored cyber actors since at least May 2021 to target Healthcare and Public Health (HPH) Sector organizations.

This joint CSA provides information—including TTPs and IOCs—on Maui ransomware obtained from FBI incident response activities and industry analysis of a Maui sample. The FBI, CISA, and Treasury urge HPH Sector organizations as well as other critical infrastructure organizations to apply the recommendations in the Mitigations section of this CSA to reduce the likelihood of compromise from ransomware operations. Victims of Maui ransomware should report the incident to their local FBI field office or CISA.

The FBI, CISA, and Treasury highly discourage paying ransoms as doing so does not guarantee files and records will be recovered and may pose sanctions risks. Note: in September 2021, Treasury issued an updated advisory highlighting the sanctions risks associated with ransomware payments and the proactive steps companies can take to mitigate such risks. Specifically, the updated advisory encourages U.S. entities to adopt and improve cybersecurity practices and report ransomware attacks to, and fully cooperate with, law enforcement. The updated advisory states that when affected parties take these proactive steps, Treasury's Office of Foreign Assets Control (OFAC) would be more likely to resolve apparent sanctions violations involving ransomware attacks with a non-public enforcement response.

For more information on state-sponsored North Korean malicious cyber activity, see CISA's North Korea Cyber Threat Overview and Advisories webpage.

Download the PDF version of this report: pdf, 553 kb.
Click here for STIX.

FBI IC3 Industry Alerts: Q3 2022

The FBI Alerts issued in conjunction with CISA and can be found in the above section of this report. This section contains FBI alerts that were issued independently during the quarter.

National Security Agency/ Central Security Service (NSA-CSS) Advisories and Guidance: Q3 2022

Control System Defense: Know the Opponent

Operational technology/industrial control system (OT/ICS) assets that operate, control, and monitor day-to-day critical infrastructure and industrial processes continue to be an attractive target for malicious cyber actors. These cyber actors, including APT groups, target OT/ICS assets to achieve political gains, economic advantages, or destructive effects. Because OT/ICS systems manage physical operational processes, cyber actors' operations could result in physical consequences, including loss of life, property damage, and disruption of National Critical Functions.

OT/ICS devices and designs are publicly available, often incorporate vulnerable information technology (IT) components, and include external connections and remote access that increase their attack surfaces. In addition, a multitude of tools are readily available to exploit IT and OT systems. As a result of these factors, malicious cyber actors present an increasing risk to ICS networks.

Traditional approaches to securing OT/ICS do not adequately address current threats to those systems. However, owners and operators who understand cyber actors' tactics, techniques, and procedures (TTPs) can use that knowledge when prioritizing hardening actions for OT/ICS.

This joint Cybersecurity Advisory, which builds on previous NSA and CISA guidance to stop malicious ICS activity and reduce OT exposure, describes TTPs that malicious actors use to compromise OT/ICS assets. It also recommends mitigations that owners and operators can use to defend their systems. NSA and CISA encourage OT/ICS owners and operators to apply the recommendations in this CSA.

Iranian Islamic Revolutionary Guards - Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations

This joint Cybersecurity Advisory (CSA) is the result of an analytic effort among the FBI, the CISA, the National Security Agency (NSA), U.S. Cyber Command (USCC) - Cyber National Mission Force (CNMF), the Department of the Treasury (Treasury), the ACSC, the Canadian Centre for Cyber Security (CCCS), and the United Kingdom's National Cyber Security Centre (NCSC) to highlight continued malicious cyber activity by APT actors that the authoring agencies assess are affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC). Note: The IRGC is an Iranian Government agency tasked with defending the Iranian Regime from perceived internal and external threats. Hereafter, this advisory refers to all the coauthors of this advisory as "the authoring agencies."

This advisory updates joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities, which provides information on these Iranian government-sponsored APT actors exploiting known Fortinet and Microsoft Exchange vulnerabilities to gain initial access to a broad range of targeted entities in furtherance of malicious activities, including ransom operations. The authoring agencies now judge these actors are an APT group affiliated with the IRGC.

Since the initial reporting of this activity in the FBI Liaison Alert System (FLASH) report APT Actors Exploiting Fortinet Vulnerabilities to Gain Access for Malicious Activity from May 2021, the authoring agencies have continued to observe these IRGC-affiliated actors exploiting known vulnerabilities for initial access. In addition to exploiting Fortinet and Microsoft Exchange vulnerabilities, the authoring agencies have observed these APT actors exploiting VMware Horizon Log4j vulnerabilities for initial access. The IRGC-affiliated actors have used this access for follow-on activity, including disk encryption and data extortion, to support ransom operations.

The IRGC-affiliated actors are actively targeting a broad range of entities, including entities across multiple U.S. critical infrastructure sectors as well as Australian, Canadian, and United Kingdom organizations. These actors often operate under the auspices of Najee Technology Hooshmand Fater LLC, based in Karaj, Iran, and Afkar System Yazd Company, based in Yazd, Iran. The authoring agencies assess the actors are exploiting known vulnerabilities on unprotected networks rather than targeting specific targeted entities or sectors.

This advisory provides observed tactics, techniques and IOCs, that the authoring agencies assess are likely associated with this IRGC-affiliated APT. The authoring agencies urge organizations, especially critical infrastructure organizations, to apply the recommendations listed in the Mitigations section of this advisory to mitigate risk of compromise from these IRGC- affiliated cyber actors.

For a downloadable copy of IOCs, see AA22-257A.stix.

For more information on Iranian state-sponsored malicious cyber activity, see CISA's Iran Cyber Threat Overview and Advisories webpage and the FBI's Iran Threat webpage.

Announcing the Commercial National Security Algorithm Suite 2.0

The need for protection against a future deployment of a cryptanalytically relevant quantum computer (CRQC) is well documented. That story begins in the mid-1990s when Peter Shor discovered a CRQC would break public-key systems still used today. Continued progress in quantum computing research by academia, industry, and some governments suggests that the vision of quantum computing will ultimately be realized. Hence, now is the time to plan, prepare, and budget for an effective transition to quantum-resistant (QR) algorithms, to assure continued protection of National Security Systems (NSS) and related assets.

This advisory notifies NSS owners, operators, and vendors of future requirements for QR algorithms for NSS. These algorithms (also referred to as post-quantum algorithms) are analyzed as being secure against both classical and quantum computers. They are an update to those in the Commercial National Security Algorithm Suite (referred to as CNSA 1.0, the algorithms currently listed in CNSSP 15, Annex B). NSA will reference this update as CNSA Suite 2.0, and any future updates will modify the version number.

NSA is providing this advisory in accordance with authorities detailed in NSD-42, NSM8, NSM-10, CNSSP 11, and CNSSP 15. Its direction applies to all NSS use of public cryptographic algorithms (as opposed to algorithms NSA developed), including those on all unclassified and classified NSS. Using any cryptographic algorithms the National Manager did not approve is generally not allowed, and requires a waiver specific to the algorithm, implementation, and use case. In accordance with CNSSP 11, software and hardware providing cryptographic services require National Information Assurance Partnership (NIAP) or NSA validation in addition to meeting the requirements of the appropriate version of CNSA.

The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ

CNSA 2.0 is the suite of QR algorithms approved for eventual NSS use. CNSA 2.0 algorithms will be required for all products that employ public-standard algorithms in NSS, whether a future design or currently fielded. Any usage of Suite B or CNSA 1.0 algorithms will be required to transition to CNSA 2.0 usage.

NSA intends that all NSS will be quantum-resistant by 2035, in accordance with the goal espoused in NSM-10. NSA relies upon NIST-approved commercial cryptography for commercial solutions. After NIST has finalized the standards associated with CNSA 2.0, NSA will update CNSSP 15. New cryptographic developments will be required to support CNSA 2.0 algorithms as an option once appropriate standards for the given technology are in place, and all appropriate system components should be configured to prefer CNSA 2.0 algorithms. As products mature, those components should be configured to accept only CNSA 2.0 algorithms. NSA will provide guidance and updated protection profiles as industry develops the appropriate standards because product lines may develop at different speeds. CNSA 1.0 algorithms will continue to be used until current solutions can operate in a CNSA 2.0 mode.

NSA chose algorithms selected for standardization by the National Institute of Standards and Technology (NIST), the U.S. Government lead for commercial algorithm approval. NSA believes they offer optimal performance for given NSS security requirements.

NSA performed its own analysis of CNSA 2.0 algorithms and considers them appropriate for long-term use in protecting the varied missions of U.S. NSS. NSA makes no specific claims regarding the performance of these algorithms against specific security metrics.

NSA intends to provide implementation guidance for CNSA 2.0 algorithms, but has not determined where it will publish the guidance. NSA makes CNSA 2.0 requirements, anticipated timing, and this related FAQ widely available to assist NSS owners and operators in their transition planning and to inform industry of NSS requirements. Even NSS systems that are in use will need to be upgraded in a timely fashion unless the system receives a waiver through the approved process.

High-grade equipment will follow the guidance in CJCSN 65104 and CNSSAM 01-07NSM5. Commercial equipment will follow CNSA 1.0 until the transition mandated by CNSSP 156, expected to occur sometime between 2025 and 2030, depending on equipment type. In accordance with NSM-10, QR algorithms should be implemented in mission systems only when the National Information Assurance Partnership (NIAP) has validated them.

NIST standardized stateful hash-based signatures in NIST SP 800-2087. This standard also provides references to other technical documentation on the topic. NSA recommends using Federal Information Processing Standards (FIPS)-validated hashbased signatures to protect NSS in the specialized scenarios outlined in the standard— e.g., for firmware signing and software signing. NSA's preferred parameter set is Section 4.2, LMS with SHA-256/192.

Securing the Software Supply Chain

Cyberattacks are conducted via cyberspace and target an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information.

Recent cyberattacks such as those executed against SolarWinds and its customers, and exploits that take advantage of vulnerabilities such as Log4j, highlight weaknesses within software supply chains, an issue which spans both commercial and open source software and impacts both private and government enterprises. Accordingly, there is an increased need for software supply chain security awareness and cognizance regarding the potential for software supply chains to be weaponized by nation state adversaries using similar TTPs.

In response, the White House released an Executive Order on Improving the Nation's Cybersecurity (EO 14028). EO 14028 establishes new requirements to secure the federal government's software supply chain. These requirements involve systematic reviews, process improvements, and security standards for both software suppliers and developers, in addition to customers who acquire software for the Federal Government.

Similarly, the Enduring Security Framework2 (ESF) Software Supply Chain Working Panel has established this guidance to serve as a compendium of suggested practices for developers, suppliers, and customer stakeholders to help ensure a more secure software supply chain. This guidance is organized into a three part series: Part 1 of the series focuses on software developers; Part 2 focuses on software suppliers; and Part 3 focuses on software customers.

Customers (acquiring organizations) may use this guidance as a basis of describing, assessing, and measuring security practices relative to the software lifecycle. Additionally, suggested practices listed herein may be applied across the acquisition, deployment, and operational phases of a software supply chain.

The software supplier (vendor) is responsible for liaising between the customer and software developer. Accordingly, vendor responsibilities include ensuring the integrity and security of software via contractual agreements, software releases and updates, notifications, and mitigations of vulnerabilities. This guidance contains recommended best practices and standards to aid suppliers in these tasks.

This document will provide guidance in line with industry best practices and principles, which software developers are strongly encouraged to reference. These principles include security requirements planning, designing software architecture from a security perspective, adding security features, and maintaining the security of software and the underlying infrastructure (e.g., environments, source code review, testing).

Kubernetes Hardening Guide

Kubernetes® is an open-source system that automates the deployment, scaling, and management of applications run in containers, and is often hosted in a cloud environment. Using this type of virtualized infrastructure can provide several flexibility and security benefits compared to traditional, monolithic software platforms. However, securely managing everything from microservices to the underlying infrastructure introduces other complexities. This report is designed to help organizations handle Kubernetes-associated risks and enjoy the benefits of using this technology.

Three common sources of compromise in Kubernetes are supply chain risks, malicious threat actors, and insider threats. Supply chain risks are frequently challenging to mitigate and can arise in the container build cycle or infrastructure acquisition. Malicious threat actors can exploit vulnerabilities and misconfigurations in components of the Kubernetes architecture, such as the control plane, worker nodes, or containerized applications. Insider threats can be administrators, users, or cloud service providers. Insiders with special access to an organization's Kubernetes infrastructure may be able to abuse these privileges.

This guide describes the security challenges associated with setting up and securing a Kubernetes cluster. It includes strategies for system administrators and developers of National Security Systems, helping them avoid common misconfigurations and implement recommended hardening measures and mitigations when deploying Kubernetes.

This guide details the following mitigations:

- Scan containers and pods for vulnerabilities or misconfigurations.
- Run containers and pods with the least privileges possible.
- Use network separation to control the amount of damage a compromise can cause.
- Use firewalls to limit unneeded network connectivity, and use encryption to protect confidentiality.
- Use strong authentication and authorization to limit user and administrator access, as well as to limit the attack surface.
- Capture and monitor audit logs so that administrators can be alerted to potential malicious activity.
- Periodically review all Kubernetes settings and use vulnerability scans to ensure risks are appropriately accounted for, and security patches are applied.

DOD Microelectronics: Levels of Assurance Definitions and Applications

This document describes a consistent and measurable approach to addressing assurance risks in the fabrication of custom microelectronic components (CMC), comprised of Application Specific Integrated Circuits (ASIC), Field Programmable Gate Arrays (FPGA), and other microelectronic devices whose function is custom or configurable. This document defines three levels of hardware assurance and the steps necessary to apply them in the protection of custom microelectronic parts used in DoD systems.

For the purpose of this document, the Defense Acquisition University (DAU) definition for hardware assurance (HwA) has been adapted to the following:

"An evidence-supported level of confidence that a CMC device and its configuration do not contain unexpected characteristics or exhibit unintended behaviors due to the influence of an adversary or known vulnerabilities that will enable an adversary to influence the system's behavior. These characteristics or behaviors could range from degraded reliability to denial of service or to complex functional changes."

Consistent with this definition, the Joint Federated Assurance Center (JFAC) has identified three levels of HwA to be applied by DoD programs to their top-level system and its critical components.

Once the system is categorized at the appropriate level of assurance (LoA), the respective CMC is further analyzed to determine potential threats to the manufacturing process. The threats are defined by two characteristics at each level: cost and utility. The following table documents the cost and utility characteristics at each LoA.

After CMC LoAs have been determined by the program, the program should utilize JFAC best practice guides for the relevant assurance level to identify the threats present at that level and effective techniques for mitigating each. These mitigations can be incorporated directly into a Program Protection Plan (PPP). In this document, CMC products are defined to include the full range of devices containing reprogrammable digital logic that can implement arbitrary digital functions and fully custom integrated circuits. This includes devices marketed as field programmable gate arrays (FPGAs), such as complex programmable logic devices (CPLD), and system-on-chip (SoC) FPGAs.

The Infoblox Threat Intelligence Group

With over 50 years of combined experience, the Infoblox Threat Intelligence Group creates, aggregates and curates information on threats to provide actionable intelligence that is high-quality, timely, and reliable. Threat information from Infoblox filters out false positives and gives you the information you need to block the newest threats and to maintain a unified security policy across the entire security infrastructure of your organization.

Infoblox Threat Intelligence

Infoblox Threat Intelligence provides timely and accurate data that helps protect organizations against cyber threats. Our data is curated from more than two dozen partners, and our key sources include leading threat intelligence providers, government agencies, universities, and the Department of Homeland Security's Automated Indicator Sharing program. Infoblox Threat Intelligence provides a single platform for managing and distributing all of our licensed data sets within an organization's ecosystem.

Powered by the
Infoblox Threat Intelligence Group

Infoblox is the leader in modern, cloud-first networking and security services. More than 12,000 customers, including over 70 percent of the Fortune 500, rely on Infoblox to scale, simplify and secure their hybrid networks to meet the modern challenges of a cloud-first world.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com

Infoblox