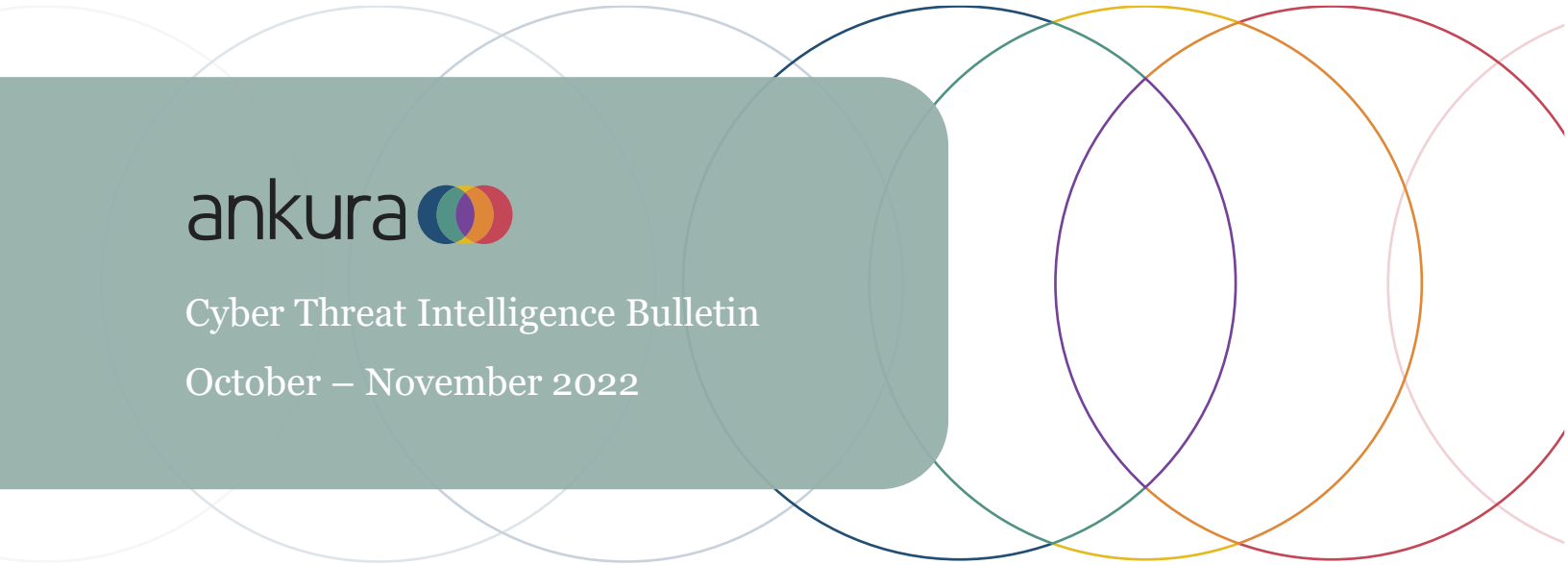

ankura

Cyber Threat Intelligence Bulletin

October – November 2022

Washington, DC
2000 K Street NW, 12th Floor
Washington, DC, United States 20006
+1.202.797.1111

Ankura Incident Response Services
Incident@ankura.com | 24/7 Assistance

TABLE OF CONTENTS

Executive Summary

Ankura's Cyber Threat Investigations and Expert Services (CTIX) team has compiled details of current cyber trends within the last sixty (60) days. This summary is intended to provide a medium depth of knowledge to high-level executives, technical analysts, and everyday readers who are looking to gain a deeper understanding of current, global threats.

This report will discuss the following in detail:

- Threat actors compromised approximately 15,000 WordPress sites as part of a massive search engine optimization (SEO) campaign.
- Though impersonation and inauthentic accounts are not new to the Twitter landscape, Twitter Blue, Twitter's newest verification system, enabled increases in impersonation and phishing campaigns.
- A new ransomware strain dubbed "Somnia" is being deployed in multiple Ukrainian organizations by the Russian hacktivist group "From Russia with Love" (FRwL).
- TeamTNT, a threat group that primarily targets cloud and compartmentalized environments to deploy infectious cryptocurrency miners, has recently pinged several endpoints, showing activity from the group after reported shutdown in 2021.

COORDINATED SEO POISONING REDIRECT CAMPAIGN HACKED THOUSANDS OF WEBSITES

- Massive SEO redirect campaign compromises almost 15,000 WordPress sites.
- Redirects send the user to an actor-controlled sites like Q&A forums.
- As multiple IPs from all over the world interact with the compromised site, the websites ranking in Google Search is increased, leading even more unsuspecting users to the redirected domain.

Summary

Malicious hackers have been observed conducting a massive and sophisticated search engine optimization (SEO) campaign, compromising approximately 15,000 WordPress websites between September and November of 2022. The purpose of the campaign is to socially engineer a multitude of users into visiting and interacting with the malicious sites to boost the pages' rankings in Google's own index. The more engagement a website receives, the higher the page's ranking and chance of search engines to recommend that site to users.

The campaign was analyzed by researchers from the website security and protection platform Sucuri[1]. According to the report, hackers are modifying WordPress PHP files in websites with "ois[.]is" malware, embedding them with malicious redirect scripts that bring the user to a fake Q&A discussion forum created by the hackers, instead of the page the user intended to visit.[2] Unlike SEO spam campaigns where actors use their websites to rank content that wouldn't rank otherwise, SEO redirect campaigns aim to funnel their unsuspecting victims away from the intended websites to an actor-controlled site[3]. The sites themselves appear to be very similar in design, utilizing common templates with low-quality text, often written in Arabic. It also appears that the sites have been created using a form of automation, as the sites utilize the same Q&A pattern built using the Question2Answer (Q2A) open-source Q&A platform. This would explain the poor syntax that appears to be uniform across the sites. Some of the infected websites have multiple subdomains, with an average of over one hundred (100) infected files for each website. The most commonly affected files are core WordPress files, and ois[.]is also appears in previously infected malicious ".php" files.

[1] https://blog.sucuri.net/2022/11/massive-ois-is-black-hat-redirect-malware-campaign.html
[2] https://blog.sucuri.net/2022/11/massive-ois-is-black-hat-redirect-malware-campaign.html
[3] https://blog.sucuri.net/2020/05/malicious-redirects.html

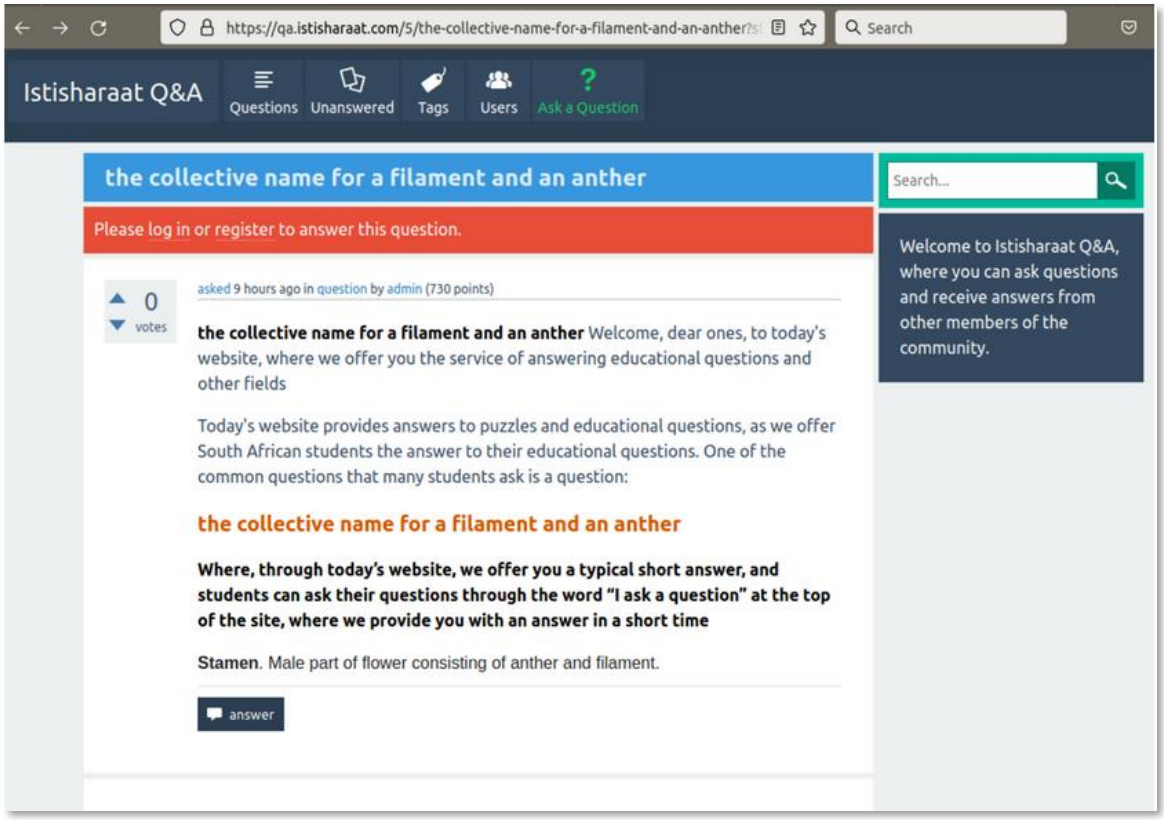

Figure 1. Redirect to a Q&A Forum[4]

When a victim accesses an infected page, the first action "ois[.]is" carries out is to verify that the user isn't a WordPress administrator. If the cookie "wordpress_logged_in" is present, the redirect will not occur. The exclusion of logged in users is an evasive technique to avoid suspicion, since the longer a page can remain up and undetected, the more engagement it will get, leading to a higher Google Search ranking. If the cookie isn't present, the malware always redirects to "logo.png" files, with the simplest version having a single redirect and more complex versions having several.

```
$ckUjYggTf = 0;
foreach($_COOKIE as $vUjUnHvOOoO => $vvvUjUnHvOOoO){
  if (strstr(strval($vUjUnHvOOoO), 'wordpress_logged_in')){
    $ckUjYggTf = 1;
    break;
  }
}

if($ckUjYggTf == 0 && !strstr(strval($_SERVER['REQUEST_URI']), 'wp-login.php')){
```

Figure 2. Validating if the user is an admin or on the login page[5]

[4] https://blog.sucuri.net/2022/11/massive-ois-is-black-hat-redirect-malware-campaign.html
[5] https://blog.sucuri.net/2022/11/massive-ois-is-black-hat-redirect-malware-campaign.html

This SEO redirect campaign is simply laying the groundwork for a much more volatile campaign in the future. Once the high ranking in Google search is achieved, the threat actors could move from malicious redirects to destructive malware droppers hosting malware like infostealers, cryptostealers, ransomware, and spyware. Interestingly, some of the sites with second level domains contain “ads.txt” files, indicating that there was an attempt to place AdSense advertisements from Google. However, the profits from AdSense paled in comparison to the scraped content used to generate redirect sites.

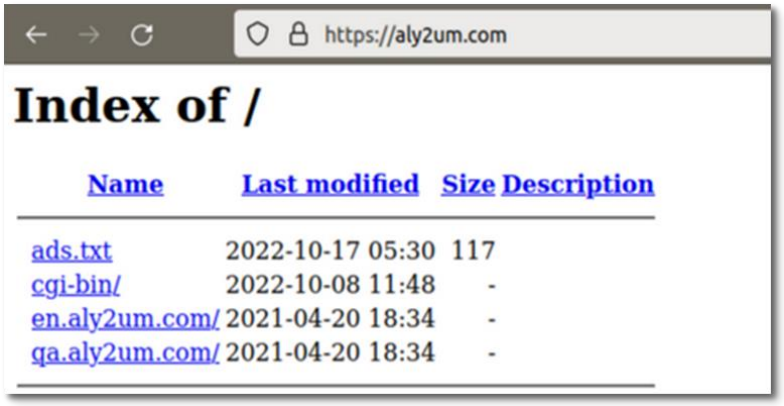

Figure 3. “ads.txt” file for Google AdSense[6]

It should be noted that most of the malicious sites are hidden behind CloudFlare proxy servers, in which the Sucuri researchers were unable to learn more about the operators facilitating the campaign. At this time, it cannot be noted what the vector for compromise is; however, researchers suspect that the threat actors gained access by exploiting very prevalent WordPress vulnerabilities. WordPress developers and administrators should investigate their sites to identify if they’ve been compromised from this campaign. Sucuri recommends that administrators query their file systems to perform a core file integrity check, which will identify files with the “ois[.]is” malware. Arbitrary or spoofed “.htaccess” files or spam “.html” files should also be monitored for, as they are often paired with “ois[.]is”. To mitigate being compromised by this campaign in the future, administrators are recommended to “change all administrator and access point passwords (such as FTP accounts, cPanel, hosting, etc)”, as well as secure their “wp-admin” panel with two-factor authentication (2FA).[7]

[6] https://blog.sucuri.net/2022/11/massive-ois-is-black-hat-redirect-malware-campaign.html
[7] https://blog.sucuri.net/2022/11/massive-ois-is-black-hat-redirect-malware-campaign.html

RECENT CYBER THREATS SURROUNDING TWITTER

- Elon Musk became the owner and CEO of Twitter on October 27, 2022, and created a new verification system called Twitter Blue on November 9, 2022.
- Impersonation and inauthentic account services/tools found on dark web forums are not new to the landscape but can be utilized further with the platform's recent changes.
- New phishing campaigns are also emerging and taking advantage of Twitter Blue.

Summary

Various researchers have begun noticing an increase in phishing campaigns targeting Twitter user credentials as well as an overall presence of threat activity surrounding Twitter following the acquisition of Twitter by Elon Musk. Elon Musk became the owner and CEO of Twitter on October 27, 2022, after making an initial bid to buy Twitter at $54.20 per share (which totaled to $44 billion) on April 13, 2022.[8] Soon after Musk's take over, various changes were implemented to the website as well as the company as a whole. Twitter launched a new verification system on November 9, 2022, that enabled users to purchase Twitter Blue for $8, which would provide a blue checkmark to their profile.[9] Previously, having a blue verification checkmark indicated that the user had passed certain verification tests and requirements with Twitter and served as a means to verify the owner of the account. With the old criteria, these checkmarks were given to government officials, celebrities, journalists, organizations, and more. With the new criteria through Twitter Blue, any user can now pay for their status symbol on the platform. Due to users abusing this privilege by impersonating brands and trustworthy public figures, the Twitter Blue subscriptions were paused two (2) days after the service was introduced.[10] On November 18, 2022, Musk stated that accounts less than ninety (90) days old could not sign up for Twitter Blue and on November 21, 2022, Musk explained that Twitter Blue would continue to be paused for some time until there is "high confidence of stopping impersonation."[11]

Impersonating and inauthentic accounts are not new to Twitter. Cybersixgill recently reported that a "significant portion of inauthentic Twitter accounts may have been built with tools and services found on the deep and dark web."[12] These tools and services were categorized into two (2) types: account amplification and account takeover. Both types were advertised in various postings on forums for a range of prices. Account amplification allows users to purchase bots for automated actions, services to add mass followers to an account, and pre-built accounts with mass followings.[13] One example contained a posting for a Twitter bot that advertised "mass subscriptions, likes, retweets, comments, and tweets, as well as the ability to change the profile's username, name, and description."[14]

[8] https://www.npr.org/2022/10/27/1131378869/twitter-elon-musk-timeline
[9] https://www.searchenginejournal.com/elon-musks-twitter-takeover-a-timeline-of-events/470927/
[10] https://www.searchenginejournal.com/elon-musks-twitter-takeover-a-timeline-of-events/470927/
[11] https://www.searchenginejournal.com/elon-musks-twitter-takeover-a-timeline-of-events/470927/
[12] https://news.cybersixgill.com/twitter-has-a-massive-dark-web-problem/
[13] https://news.cybersixgill.com/twitter-has-a-massive-dark-web-problem/
[14] https://news.cybersixgill.com/twitter-has-a-massive-dark-web-problem/

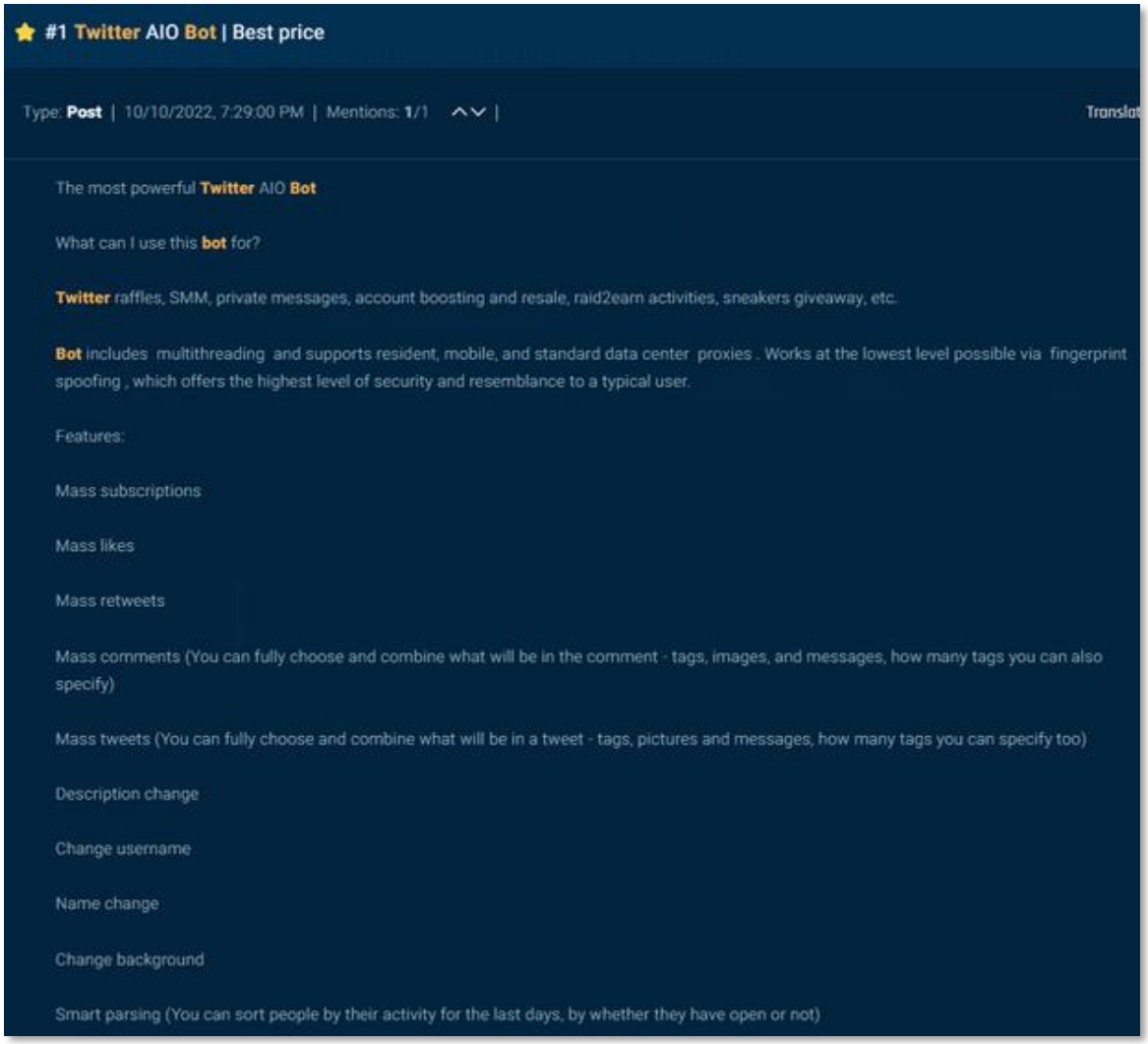

Figure 1: Account Amplification Forum Posting[15]

Account takeover allows for users to acquire a different user's account through credential-stuffing tools and combolists, the sale of validated Twitter credentials, hack-for-hire services, and scraped databases for social engineering.[16] One example advertised Twitter logs for sale. Logs are highly sought out by actors and can be obtained from credential stuffing as well as access markets, which "sell access to or data stolen from infected machines" and can include cookies, system data and IP information.[17] Cybersixgill emphasized that "out of the over 2,146,000 compromised machines sold on access markets over the last year, a whopping 435,000 (20.3%) included access to a Twitter account."[18]

[15] https://news.cybersixgill.com/twitter-has-a-massive-dark-web-problem/
[16] https://news.cybersixgill.com/twitter-has-a-massive-dark-web-problem/
[17] https://news.cybersixgill.com/twitter-has-a-massive-dark-web-problem/
[18] https://news.cybersixgill.com/twitter-has-a-massive-dark-web-problem/

Figure 2: Account Takeover Forum Posting[19]

Threat actors, along with the use of services and tools from dark web forums, have increased their campaigns targeting Twitter users due to the platform's recent changes. Proofpoint's Vice President of Threat Research and Detection Sherrod DeGrippo explained that actors are now using Twitter verification and Twitter Blue product lures in their phishing campaigns, such as "Twitter blue badge Billing Statement Available".[20] The campaigns are using "both Google Forms for data collection as well as URLs that redirect to actor-hosted infrastructure" and target users whose email addresses match their user handles and/or are in their Twitter biographies.[21] DeGrippo detailed that "compromised accounts can be used to spread misinformation, urge users to engage with additionally malicious content like fraudulent cryptocurrency scams, and can be used to further phishing campaigns to other users."[22] Various threat actors, including Karakurt, BlackByte, and most recently Yanluowang, have historically used Twitter to advertise their stolen data gained through data extortion and allow non-Tor users to obtain it.[23] DeGrippo emphasized that "while we historically observed occasional Twitter credential phishing using verification-related lures from cybercrime threat actors, the activity has increased in recent weeks."[24] This is not shocking as threat actors often take advantage of trending topics, but the repercussions of accounts being taken over now may have a higher risk than usual. Threat actors are constantly monitoring social media platforms for the next vulnerability to exploit and rushed changes like Twitter Blue can allow actors to slip into the scene unnoticed. Prior to the Twitter Blue verification pause, any user (threat actor or not) could gain a higher chance of projecting to an easily influenced audience for $8 and cause irresponsible damage. Cybersecurity researchers are waiting for the next round of changes in the Twitter ecosystem and how threat actors will adjust their tactics, techniques, and procedures (TTPs) to come ahead.

[19] https://news.cybersixgill.com/twitter-has-a-massive-dark-web-problem/
[20] https://techmonitor.ai/technology/cybersecurity/twitter-phishing-blue-tick-verification-elon-musk
[21] https://techmonitor.ai/technology/cybersecurity/twitter-phishing-blue-tick-verification-elon-musk
[22] https://techmonitor.ai/technology/cybersecurity/twitter-phishing-blue-tick-verification-elon-musk
[23] https://techmonitor.ai/technology/cybersecurity/twitter-hackers-elon-musk-yanluowang
[24] https://techmonitor.ai/technology/cybersecurity/twitter-phishing-blue-tick-verification-elon-musk

“FROM RUSSIA WITH LOVE”: SOMNIA RANSOMWARE OVERVIEW

- “From Russia with Love” (FRwL), a Russian hacktivist group tracked as UAC-0118, has infected various Ukrainian organizations with a new ransomware strain dubbed “Somnia.”
- Somnia ransomware is similar to wiper malware, where there are no instructions for payment to decrypt the encrypted data.

Summary

The Computer Emergency Response Team of Ukraine (CERT-UA) has confirmed that Russian hacktivist group “From Russia with Love” (FRwL) has infected multiple Ukrainian organizations with a new ransomware strain dubbed “Somnia.” FRwL has taken credit for the creation of Somnia on their Telegram channel and claimed to have deployed Somnia against tank producers in Ukraine, although this is currently unconfirmed.[25] According to the CERT-UA press release, authorities were tricked into downloading and running a file that took the appearance of the “Advanced IP Scanner” software which contained an embedded malware dubbed “Vidar.”[26]

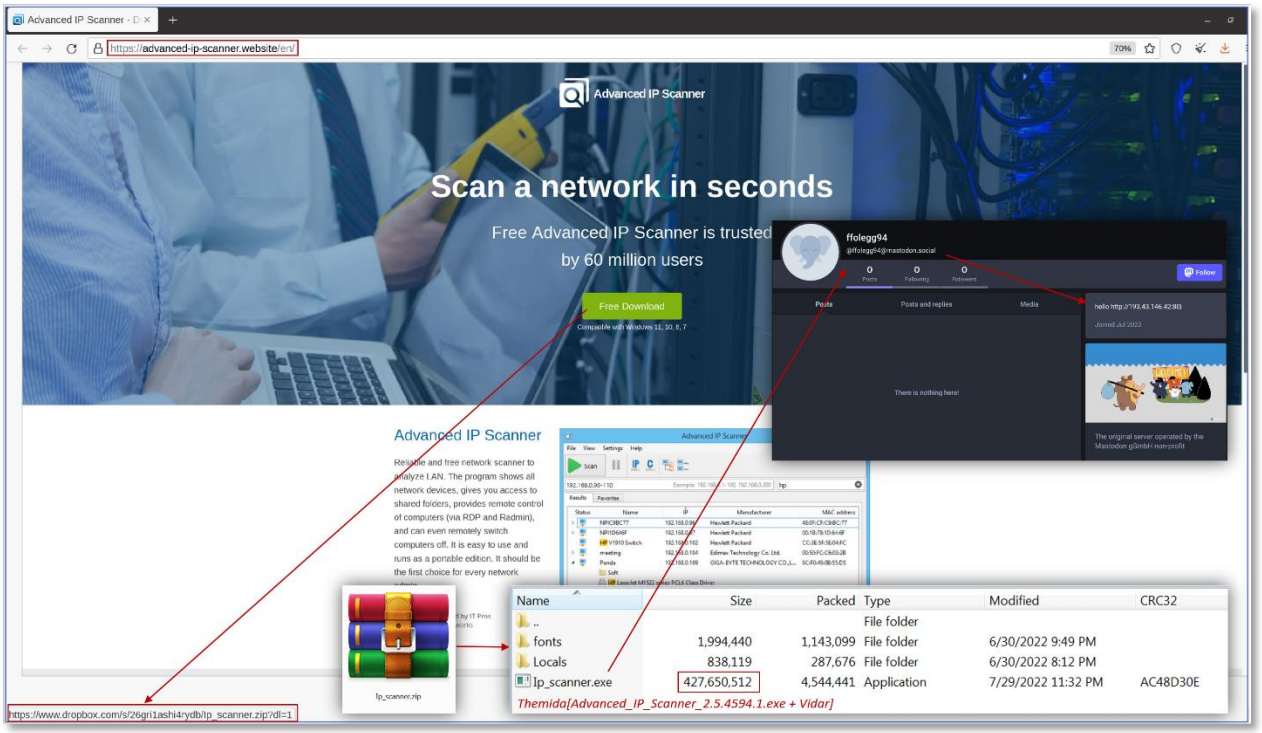

Figure 1: Example of the fake Advanced IP Scanner Program Used

It is believed that Vidar was used by an Initial Access Broker (IAB) to gain access to the target network, in which the broker transferred the desired information to FRwL to further carry out increasingly complicated cyber-attacks. Using this information, FRwL used the victim’s Telegram channel to transfer VPN configuration files to establish a direct VPN connection to the targeted network. Due to a lack of two-factor authentication (2FA), the threat actors were able to gain access to the organization’s network through an unauthorized VPN. Somnia has also been evolving since its initial deployment of Version 1 that used a 3DES encryption scheme, as the latest version uses an AES scheme to create a key that’s more difficult to

[25] https://www.bleepingcomputer.com/news/security/ukraine-says-russian-hacktivists-use-new-somnia-ransomware/
[26] https://cert.gov.ua/article/2724253

decrypt via a brute force attack[27]. The use of Somnia ransomware has the unique issue of not including any instructions for payment to decrypt the data that has been ransomed. Instead, it appears that Somnia is being deployed purely as a destructive piece of malware (occasionally called “wiper” malware) that intends to either slow down the usage of a network while decryption efforts are undertaken or to destroy the files and systems on a given network. This falls in line with Russian threat groups’ general strategy of anti-Ukrainian campaigns since before the invasion began. From Russia with Love, tracked as UAC-0118, appears to be in a position to continue expanding its campaigns and publicity. Ankura will continue to monitor situations involving Russian threat actors and the ongoing Russian invasion of Ukraine.

[27] https://securityaffairs.co/wordpress/138496/hacking/somnia-ransomware-attacks-ukraine.html

THREAT ACTOR OF THE MONTH

- TeamTNT recently pinged several Docker endpoints, showing activity from the group after its reported shutdown in 2021.
- Known WatchDog (Thief Libra) indicator of compromise uncovered in Base64 code, showing possible affiliation to the attack.
- While unconfirmed, this security event could be an indication of the return of TeamTNT, or a potential takeover by another threat organization.

Summary

After indications of a potential return to the threat landscape, TeamTNT has become a threat organization that security teams and corporations must be informed of. Active since 2019, TeamTNT has been a threat group that primarily targets cloud and compartmentalized environments, such as Docker containers and Kubernetes instances, to deploy infectious cryptocurrency miners. Alongside these cryptocurrency miners, TeamTNT threat actors have been known to utilize hefty botnets to support their cryptocurrency-based operations. However, in 2021, the group posted on their deep web site that they were ceasing operations, specifically “TeamTNT has quit()”. As of November 2022, the TeamTNT domain is unresolvable; however, several archives of the website can still be found.

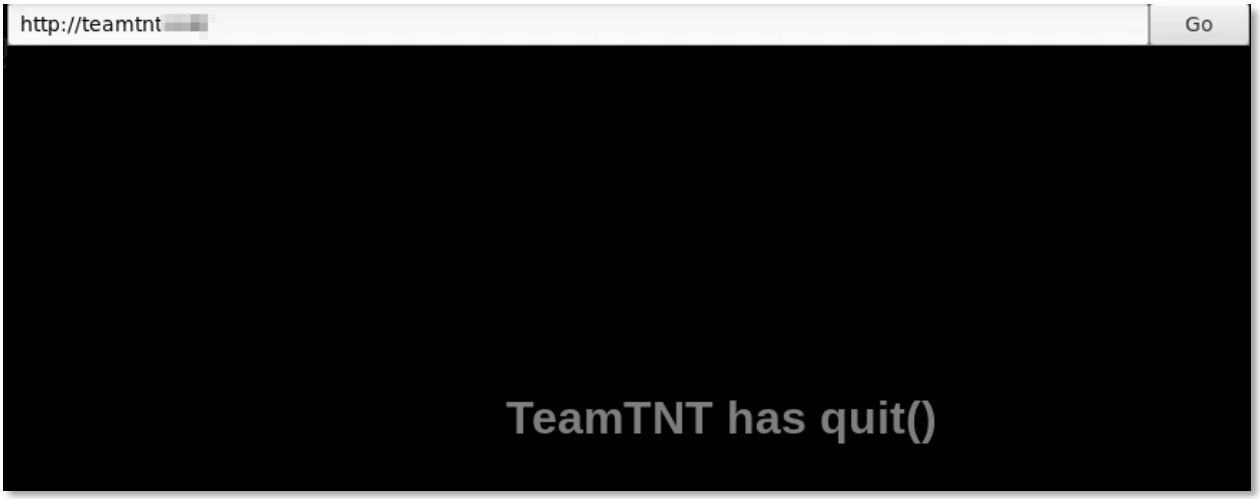

Figure 1: TeamTNT Website (December 25, 2021)

Recent observations have shown a potential return of the TeamTNT threat organization, after several indicators of compromise were observed establishing connections and making several requests to exposed Docker API endpoints.[28] The associated IP addresses to these Docker endpoints can be viewed in the *Trending IOCs* section at the conclusion of this report. In addition to these malicious indicators, attack patterns show that these undisclosed threat actors have been deploying the XMRig cryptocurrency miner. Attack flows for this infection start with the threat actors abusing Docker infrastructure to download and deploy various scripts. These scripts, including ZGrab, massscan, pnscan, and Redis, are used conjointly to act as a computer worm, eventually installing XMRig malware on the device.[29]

XMRig is a known open-source software built for harvesting cryptocurrency coins such as Monero or BitCoin. Often utilized by cryptominers, this open-source tool provides an easy way to mine cryptocurrencies and secure them to the blockchain. However, threat actors have been known to weaponize

[28] https://www.trendmicro.com/en_us/research/22/j/teamtnt-returns-or-does-it.html
[29] https://www.trendmicro.com/en_us/research/22/j/teamtnt-returns-or-does-it.html

cryptocurrency miners, creating botnets of infected machines freely mining crypto blocks on behalf of the threat actor(s). In 2021 alone, XMRig was the top cryptocurrency miner throughout the landscape, and the tenth most common crypto malware.[30] As the cryptocurrency industry continues to grow, threat actors will continue to weaponize miner applications and compromise devices to gain additional resources and hardware.

Additional malicious indicators observed in network communications from threat actor scripts/tools revealed connections to several domains, including a domain attributed to the WatchDog threat organization.[31] In operation since 2019, WatchDog (Thief Libra) is a threat group that acts similarly to TeamTNT, conducting several cryptojacking operations and credential scraping of cloud service platforms. In conjunction with similar tactics, techniques, and procedures (TTPs) of TeamTNT, WatchDog threat actors have an arsenal of repurposed cryptojacking tools harvested from several threat groups, including TeamTNT.

While still unconfirmed, it is possible that TeamTNT continues to cease operations and a copycat organization is utilizing identical TTP's to become a top threat organization in the crypto world. In the recent security event, TeamTNT IP addresses pinged Docker endpoints creating the illusion of a potential return of the group. However, the plausibility of a copycat organization remains significant after strong connections to the WatchDog threat group were uncovered. Pairing this connection, known TTPs of the WatchDog organization, and the TeamTNT domain still unresponsive, it is possible that WatchDog threat actors are utilizing former TeamTNT infrastructure to begin their next wave of cryptocurrency miner attacks. CTIX will continue to monitor activity from TeamTNT, WatchDog, and several other threat organizations worldwide, and provide additional updates accordingly.

[30] https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/xmrig-malware/
[31] https://www.trendmicro.com/en_us/research/22/j/teamtnt-returns-or-does-it.html

Trending IOCs

The following technical indicators of compromise (IOCs) are associated with monitored threat groups and/or campaigns of interest within the past sixty (60) days. IOCs can be utilized by organizations to detect security incidents more quickly and easily, as indicators may not have otherwise been flagged as suspicious or malicious.

Indicator	Type	Attribution
115.238.146[.]136	IP Address	TeamTNT & WatchDog
1.116.151[.]108	IP Address	TeamTNT & WatchDog
101.42.100[.]251	IP Address	TeamTNT & WatchDog
103.125.218[.]107	IP Address	TeamTNT & WatchDog
106.15.74[.]113	IP Address	TeamTNT & WatchDog
107.189.3[.]150	IP Address	TeamTNT & WatchDog
113.57.111[.]119	IP Address	TeamTNT & WatchDog
120.48.86[.]143	IP Address	TeamTNT & WatchDog
121.36.16[.]103	IP Address	TeamTNT & WatchDog
124.222.213[.]175	IP Address	TeamTNT & WatchDog
13.245.9[.]147	IP Address	TeamTNT & WatchDog
139.59.132[.]89	IP Address	TeamTNT & WatchDog
150.158.33[.]66	IP Address	TeamTNT & WatchDog
176.123.10[.]57	IP Address	TeamTNT & WatchDog
199.19.226[.]117	IP Address	TeamTNT & WatchDog
205.185.118[.]246	IP Address	TeamTNT & WatchDog
27.128.160[.]170	IP Address	TeamTNT & WatchDog
39.100.33[.]209	IP Address	TeamTNT & WatchDog
45.9.148[.]35	IP Address	TeamTNT & WatchDog
45.9.148[.]37	IP Address	TeamTNT & WatchDog
45.9.150[.]36	IP Address	TeamTNT & WatchDog
47.253.42[.]213	IP Address	TeamTNT & WatchDog
58.192.31[.]232	IP Address	TeamTNT & WatchDog
85.214.149[.]236	IP Address	TeamTNT & WatchDog
http://107.189.3[.]150/b2f628/cronb.sh	Domain	TeamTNT & WatchDog
http://205.185.118[.]246/b2f628//b.sh	Domain	TeamTNT & WatchDog
http://205.185.118[.]246/b2f628/cronb.sh	Domain	TeamTNT & WatchDog
http://205.185.118[.]246/bWVkaWEK/1.0.4.tar.gz	Domain	TeamTNT & WatchDog
http://205.185.118[.]246/bWVkaWEK/config.json	Domain	TeamTNT & WatchDog
http://205.185.118[.]246/bWVkaWEK/p.tar	Domain	TeamTNT & WatchDog
http://205.185.118[.]246/bWVkaWEK/xm.tar	Domain	TeamTNT & WatchDog
http://205.185.118[.]246/bWVkaWEK/zgrab	Domain	TeamTNT & WatchDog
http://205.185.118[.]246/s3f815/d/c.sh	Domain	TeamTNT & WatchDog
http://205.185.118[.]246/s3f815/d/d.sh	Domain	TeamTNT & WatchDog
http://205.185.118[.]246/s3f815/s/s.sh	Domain	TeamTNT & WatchDog

http://de.gsearch.com[.]de	Domain	TeamTNT & WatchDog
http://dk.zzhreceive[.]top/b2f628/cronb.sh	Domain	TeamTNT & WatchDog
http://global.bitmex.com[.]de	Domain	TeamTNT & WatchDog
http://gsearch.com[.]de	Domain	TeamTNT & WatchDog
http://kiss.a-dog[.]top/b2f628/b.sh	Domain	TeamTNT & WatchDog
http://kiss.a-dog[.]top/t.sh	Domain	TeamTNT & WatchDog
http://oracle.zzhreceive[.]top	Domain	TeamTNT & WatchDog
http://oracle.zzhreceive[.]top/b2f628/cronb.sh	Domain	TeamTNT & WatchDog
http://projectbluebeam.anondns[.]net	Domain	TeamTNT & WatchDog
http://zzhreceive.anondns[.]net	Domain	TeamTNT & WatchDog