deepwatch

Cyber Intel Brief

January 15 - 21, 2022

See Threats. Stop Breaches. Together

*Prepared by **deepwatch Threat Intel Team***

Table of Contents

Quick Look

Phishing | **Phishers Lure Victims with Fake Invites to Bid on Nonexistent Federal Projects**
3 minutes 30 seconds reading time

- **Key Takeaway:**
  In a recent blog post, INKY details their analysis of a phishing campaign they observed that impersonated the United States Department of Labor (DoL) detected in the second half of 2021. These phishing emails attempted to fool recipients to submit bids for "ongoing government projects" and claimed to be from a senior DoL employee responsible for procurement. Each email had a very elaborate 3 page PDF attached. The threat actors also impersonated the DoL's website by copying and pasting the HTML and CSS code.
- **deepwatch Threat Intel Outlook:**
  deepwatch Threat Intel Team estimates with **high confidence** that threat actors will continue to impersonate high-profile and known brands. The best practice to defend against any phishing campaign is to train end-users to identify and report suspicious emails for further analysis and not enter credentials in unknown and never used before login screens.

Threat Actors | **Earth Lusca Employs Sophisticated Infrastructure, Varied Tools and Techniques**
3 minutes 30 seconds reading time

- **Key Takeaway:**
  Trend Micro recently published a technical brief that includes the activities, the tools it employs in attacks, and the infrastructure it uses, of the threat actor Earth Lusca. The group's major purpose appears to be cyberespionage: among its victims are government and educational institutions, religious movements, pro-democracy and human rights organizations in Hong Kong, Covid-19 research organizations, and the media, among others.
- **deepwatch Threat Intel Outlook:**
  deepwatch Threat Intel Team assesses with **moderate confidence** that Earth Lusca will continue to target customers via social engineering tactics like spear-phishing or watering hole attacks as well as exploiting vulnerabilities in public-facing applications.

Malicious Infrastructure | **2021 Adversary Infrastructure Report**
4 minutes reading time

- **Key Takeaway:**
  Throughout 2021, the Insikt Group of Recorded Future undertook a study of malicious command and control (C2) infrastructure discovered through proactive scanning and collecting methods. Recorded Future's analysis revealed that families of post-exploitation frameworks and botnet infrastructure were the most often observed. They also discovered that Cobalt Strike Team Servers were the most often detected C2 controllers, accounting for 23.7 percent of all C2 servers found.
- **deepwatch Threat Intel Outlook:**
  deepwatch Threat Intel Team estimates with **moderate confidence** that C2 servers will be further insulated and modified in 2022 to prevent discovery. Therefore, to mitigate the risk associated with malicious C2 servers, the Threat Intel Team recommends that customers patch systems and software as soon as possible, have a reliable and tested backup method, and finally, implement multi-factor authentication on exposed remote access systems, such as Remote Desktop, Citirix, and VPN gateways. If possible, implementing a Geo-blocking strategy is recommended as data points suggest the C2 IPs are being hosted in countries that organizations may not have business interactions such as Russia or Romania.

Quick Look

Ransomware | New Ransomware Spotted: White Rabbit and Its Evasion Tactics
2 minutes 45 seconds reading time

- **Key Takeaway:**
  Trend Micro analyzed a new ransomware family dubbed White Rabbit with indications that it may be linked to the threat actor FIN8. White Rabbit uses a tactic that is also employed by Egregor, password protecting its payload binary. In addition, the links to FIN8 are derived from the use of a URL and a never-before-seen variant of the backdoor Badhatch.
- **deepwatch Threat Intel Outlook:**
  deepwatch Threat Intel Team judges with **moderate confidence** that the threat actors behind White Rabbit are still developing the ransomware family. In light of this new ransomware family, the best defense is observing malicious activities before the execution of the encryption script. In addition, implement multi-factor authentication on exposed servers, develop an end-user training program, and finally, implement a strong password policy.

Vulnerability | Mixed Messages: Busting Box's MFA Methods
3 minutes 45 seconds reading time

- **Key Takeaway:**
  Varonis Threat Labs uncovered a means to overcome multi-factor authentication Box accounts that use an SMS code for login verification. A threat actor might use stolen credentials to breach an organization's Box account and exfiltrate sensitive data without having access to the victim's phone if they used this technique.
- **deepwatch Threat Intel Outlook:**
  deepwatch Threat Intel Team assesses with **moderate confidence** that threat actors are likely to use this technique to access customer networks. Therefore, the Threat Intel Team recommends that customers limit access to sensitive data and monitor the ingress and egress of sensitive data. By doing so, data exfiltration as a result of a perimeter bypass is considerably reduced.

Exploited Vulnerabilities | CISA Adds 13 Known Exploited Vulnerabilities to Catalog
1 minute reading time

- **Key Takeaway:**
  CISA has added 13 new vulnerabilities to its Known Exploited Vulnerabilities Catalog. Threat actors are actively exploiting these vulnerabilities, which are common attack vectors.
- **deepwatch Threat Intel Outlook:**
  deepwatch Threat Intel Team strongly urges all customers to prioritize timely remediation of vulnerabilities featured in CISAs Known Exploited Vulnerabilities Catalog as part of their vulnerability management practice.

Best Practices | Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats
2 minutes reading time

- **Key Takeaway:**
  CISA published "CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats" in response to the recent malicious cyber incidents in Ukraine. In the CISA insights, they layout steps and guidance for organizations to aid in reducing the likelihood of a damaging cyber intrusion, steps to quickly detect a potential intrusion, steps to ensure that organization's are prepared to respond if an intrusion occurs, and finally, how to maximize resilience to a destructive cyber incident.
- **deepwatch Threat Intel Outlook:**
  deepwatch Threat Intel Team highly encourages all customers follow CISAs guidance to make immediate progress toward enhancing cybersecurity and resilience by following the actions outlined in the CISA Insights. Furthermore, the Threat Intel Team recommends customers reference CIB-21-02 for a summary on "Understanding and Mitigating Russian State-Sponsored Cyber Threats to US Critical Infrastructure."

Phishing

Phishers Lure Victims with Fake Invites to Bid on Nonexistent Federal Projects

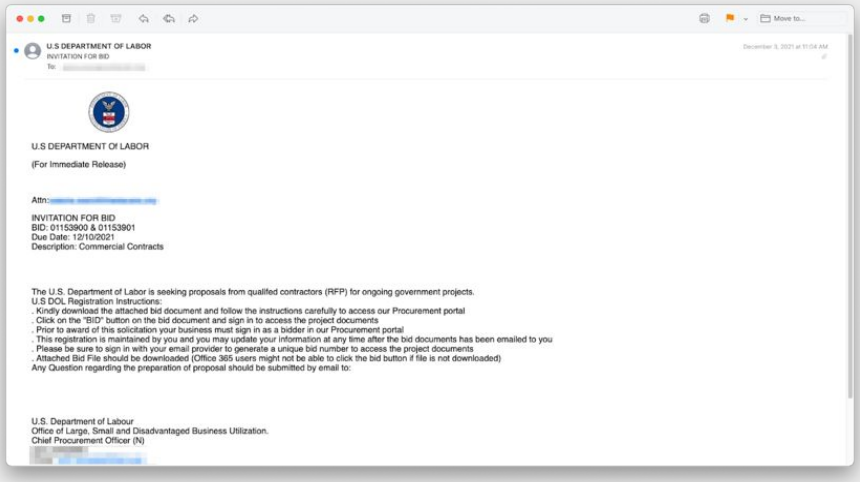
January 19, 2022 Source: *INKY* **Estimated Reading Time:** *3 minutes 30 seconds*

Key Points:

- In a recent blog post, INKY details their analysis of a phishing campaign they observed that impersonated the United States Department of Labor (DoL) detected in the second half of 2021.
- These phishing emails attempted to fool recipients to submit bids for “ongoing government projects" and claimed to be from a senior DoL employee responsible for procurement. Each email had a very elaborate 3 page PDF attached. The threat actors also impersonated the DoL’s website by copying and pasting the HTML and CSS code.
- deepwatch Threat Intel Team estimates with **high confidence** that threat actors will continue to impersonate high-profile and known brands. The best practice to defend against any phishing campaign is to train end-users to identify and report suspicious emails for further analysis and not enter credentials in unknown and never used before login screens.

Summary:
In a recent blog post, INKY details their investigation of a phishing campaign they observed that impersonated the United States Department of Labor (DoL) detected in the second half of 2021.

INKY observed that the phishing attempts came from “no-reply@dol[.]gov,” “no-reply@dol[.]com,” “dol-gov[.]com,” “dol-gov[.]us,” or “bids-dolgov[.]us.” The only legitimate domain is “dol.gov,” all the rest are spoofed to look like it is from a legitimate domain.



Source: INKY

These phishing emails attempted to fool recipients to submit bids for “ongoing government projects" and claimed to be from a senior DoL employee responsible for procurement. Each email had a very elaborate 3 page PDF attached. The threat actors spent considerable time and effort on the attachment as it had appropriate branding for DoL. Page two of the attachment had a malicious link that, when clicked, led recipients to a malicious domain that impersonated the DoL domain.

Phishing

Phishers Lure Victims with Fake Invites to Bid on Nonexistent Federal Projects

INKY observed that the phishing attempts came from “no-reply@dol[.]gov,” “no-reply@dol[.]com,” “dol-gov[.]com,” “dol-gov[.]us,” or “bids-dolgov[.]us.” The only legitimate domain is “dol.gov,” all the rest are spoofed to look like it is from a legitimate domain.

These phishing emails attempted to fool recipients to submit bids for “ongoing government projects" and claimed to be from a senior DoL employee responsible for procurement. Each email had a very elaborate 3 page PDF attached. The threat actors spent considerable time and effort on the attachment as it had appropriate branding for DoL. Page two of the attachment had a malicious link that, when clicked, led recipients to a malicious domain that impersonated the DoL domain.

Once a recipient clicked the link they were redirected to the malicious domain. The recipient was presented with a pop-up of fake instructions on how to submit a bid. The malicious domain is identical to the actual DoL website as the threat actors copied the HTML and CSS and pasted it. Email security vendors use computer vision to detect impersonated sites. Unfortunately, since there was a fake instruction pop-up, computer vision would not detect an impersonated website.

Once a user closed out the pop-up and clicked the red “Click here to bid” button presented at the bottom of the page., they were redirected to a credential harvesting form with instructions to sign in and bid using a Microsoft Office 365 or other business email account.

If a user entered invalid credentials, the site would display an incorrect credentials error. Still, the site collected the credentials and either stored them on the site or delivered them to the threat actors via another means. If the user entered the invalid credentials again, they were redirected to the actual DoL website. This is an example of the classic con-artist technique of blowing off the target. It is intended to get rid of the target, confuse them, and delay the realization that they were duped.

INKY discovered that the threat actors sent a majority of “their phishing emails from abused servers nominally controlled by a non-profit professional membership group.” In the other cases, the threat actors created domains to send initial phishing emails and host fake DoL sites.

Recapping, INKY learned that the threat actors copied the HTML and CSS of the DoL website to impersonate them, used legitimate mail servers to deliver their phishing emails, created domains that are not in threat intelligence feeds, and collected recipients credentials if they were entered into the malicious form.

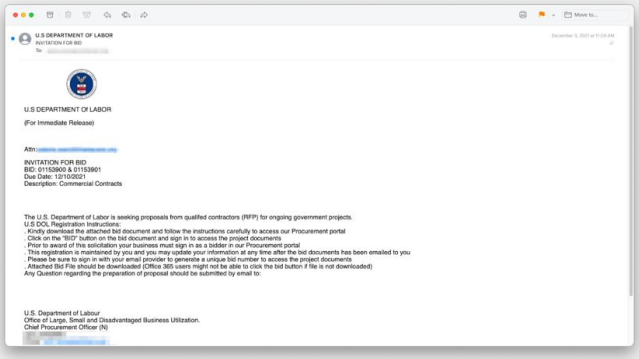
deepwatch Threat Intel Outlook:

deepwatch Threat Intel Team estimates with **high confidence** that threat actors will continue to impersonate high-profile and known brands. Threat actors will continue to take advantage of breaking news stories to trick recipients into clicking on malicious links and attachments. The best practice to defend against any phishing campaign is to train end-users to identify and report suspicious emails for further analysis and not enter credentials in unknown and never used before login screens. In addition, To prevent your email servers from being used for malicious purposes, customers should not configure them to accept and forward emails from non-local IP addresses to non-local mailboxes by unauthenticated and unauthorized users.

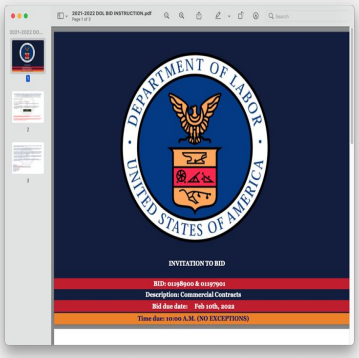
Phishing

Phishers Lure Victims with Fake Invites to Bid on Nonexistent Federal Projects

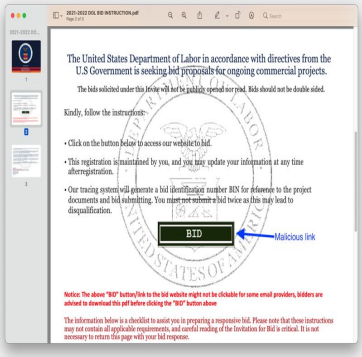
Screenshots of email, PDF attachment, and impersonated DoL website. All images sourced from INKY.



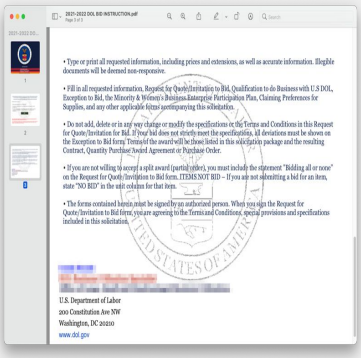
Email



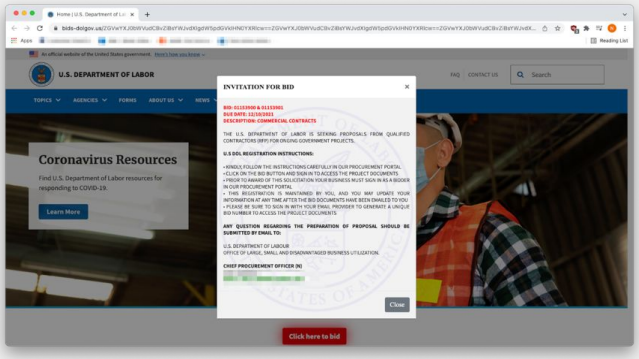
PDF Cover Page



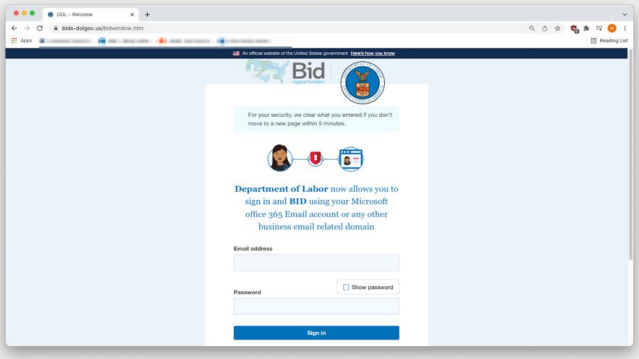
PDF Page 2



PDF Page 3



Impersonated DoL Website



Fake Login Screen

Threat Actors

Earth Lusca Employs Sophisticated Infrastructure, Varied Tools and Techniques

January 17, 2022 Source: *Trend Micro* **Estimated Reading Time:** *3 minutes 30 seconds*

Key Points:

- Trend Micro recently published a technical brief, that includes the activities, the tools it employs in attacks, and the infrastructure it uses, of the threat actor Earth Lusca.
- The group's major purpose appears to be cyberespionage: among its victims are government and educational institutions, religious movements, pro-democracy and human rights organizations in Hong Kong, Covid-19 research organizations, and the media, among others.
- deepwatch Threat Intel Team assesses with **moderate confidence** that Earth Lusca will continue to target customers via social engineering tactics like spear-phishing or watering hole attacks as well as exploiting vulnerabilities in public-facing applications.

Summary:
Trend Micro's recently published (*PDF*) "technical brief provides an in-depth look at Earth Lusca's activities, the tools it employs in attacks, and the infrastructure it uses."

Due to the use of malware like Winnti, previous research into the group's activities attributed it to other threat actors like the Winnti group, but despite some similarities, Trend Micro considers Earth Lusca to be a separate threat actor (they do have evidence, however, that the group is part of the "Winnti cluster," which is made up of different groups with the same origin country and share aspects of their TTPs).

The group's major purpose appears to be cyberespionage: among its victims are government and educational institutions, religious movements, pro-democracy and human rights organizations in Hong Kong, Covid-19 research organizations, and the media, among others. The threat actor, on the other hand, appears to also be financially driven as well, as it has targeted gaming and cryptocurrency firms.

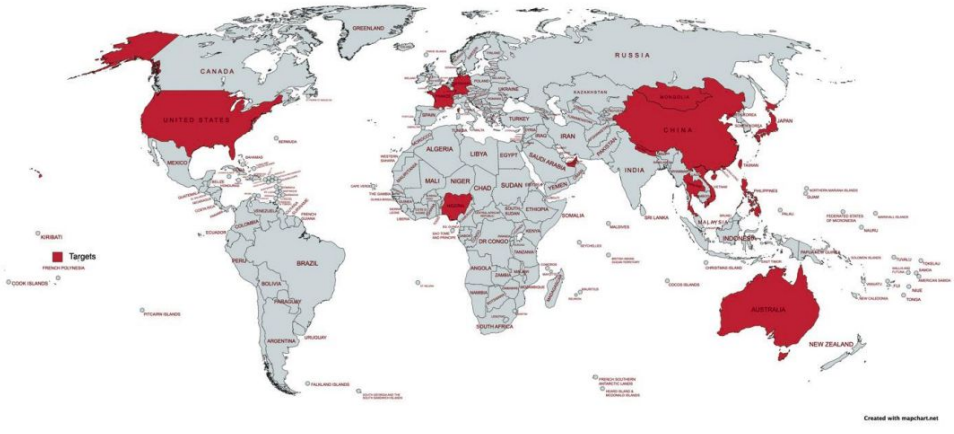


Figure 1. Affected countries and regions

Source: Trend Micro

Threat Actors

Earth Lusca Employs Sophisticated Infrastructure, Varied Tools and Techniques

Infrastructure
The infrastructure of Earth Lusca may be divided into two "clusters." The first cluster is made up of virtual private servers (VPS) that are utilized for the group's watering hole and spear-phishing activities, as well as operating as a malware command-and-control (C&C) server.

The second cluster is made up of infected computers that are running outdated open-source Oracle GlassFish Server versions. Surprisingly, in an Earth Lusca campaign, this second cluster serves as a scanning tool that looks for weaknesses in public-facing servers and creates traffic tunnels within the target's network. It also functions as a C&C server, similar to the original cluster, but this time for Cobalt Strike.

Initial Access Vectors
The group uses three main attack vectors, two of which include the social engineering tactics of spear-phishing emails and watering hole websites. Earth Lusca's third attack vector is the exploitation of vulnerabilities in its targets' public-facing programs, such as Microsoft Exchange ProxyShell and Oracle GlassFish.

Malware
Earth Lusca's arsenal includes a variety of viruses and other hacking tools. Because of its extensive post-exploitation capabilities, Cobalt Strike is one of the group's chosen tools. In this scenario, the Cobalt Strike shellcode is XOR encoded with a matching key before being delivered into the target system.

In addition to Cobalt Strike, Earth Lusca employs malware such as Doraemon, a backdoor named after a Japanese manga character that has two C&C settings: one for IP or DNS, and another for persistence through a public website URL with encrypted or clear text C&C IP addresses.

As part of its operations, the organization uses well-known malware like ShadowPad and Winnti, as well as additional tools like bitcoin miners. Trend Micro's technical brief has a more detailed list of the various malware and tools the group uses.

Earth Lusca appears to be a highly talented and skilled threat actor driven primarily by cyberespionage and financial gain, according to evidence. However, in order to attack a victim, the group still uses tried-and-true TTPs. While this has its benefits, it also implies that security best practices, such as avoiding clicking on suspicious links and patching essential public-facing applications, can help to mitigate — or even prevent — the effects of an Earth Lusca assault.

deepwatch Threat Intel Outlook:

deepwatch Threat Intel Team assesses with **moderate confidence** that Earth Lusca will continue to target customers via social engineering tactics like spear-phishing or watering hole attacks as well as exploiting vulnerabilities in public-facing applications. Trend Micro has provided a full list of MITRE ATT&CK TTPs and observables in their technical brief. The MITRE ATT&CK TTPs can be viewed here and the observables can be viewed here.

Malicious Infrastructure

2021 Adversary Infrastructure Report

January 18, 2022 Source: *Recorded Future* **Estimated Reading Time:** *4 minutes*

Key Points:

- Throughout 2021, the Insikt Group of Recorded Future undertook a study of malicious command and control (C2) infrastructure discovered through proactive scanning and collecting methods.
- Recorded Future's analysis revealed that families of post-exploitation frameworks and botnet infrastructure were the most often observed. They also discovered that Cobalt Strike Team Servers were the most often detected C2 controllers, accounting for 23.7 percent of all C2 servers found.
- deepwatch Threat Intel Team estimates with **moderate confidence** that C2 servers will be further insulated and modified in 2022 to prevent discovery. Therefore, to mitigate the risk associated with malicious C2 servers, the Threat Intel Team recommends that customers patch systems and software as soon as possible, have a reliable and tested backup method, and finally, implement multi-factor authentication on exposed remote access systems, such as Remote Desktop, Citirix, and VPN gateways. If possible, implementing a Geo-blocking strategy is recommended as data points suggest the C2 IPs are being hosted in countries that organizations may not have business interactions such as Russia or Romania.

Summary:
Recorded Future published (*PDF*) findings in their observations of over 10,000 unique command and control (C2) servers during 2021 across more than 80 families.

Last year, Recorded Future anticipated that the Sliver, Mythic, Covenant, and Octopus C2 frameworks would grow in popularity. Their most recent analysis shows that this prediction was partially correct. While the use of Covenant, Sliver, and Mythic has increased slightly, Recorded Future's visibility has demonstrated a sustained dependence on Cobalt Strike, with little adoption of other C2 frameworks.

Recorded Future found that approximately 25% (3,400) servers were not reported in open sources. They also found that during Emotet's absence in 2021, other botnets proceeded to insulate, diversify, and expand their infrastructure.

Recorded Future's analysis revealed that families of post-exploitation frameworks and botnet infrastructure were the most often observed. They also discovered that Cobalt Strike Team Servers were the most often detected C2 controllers, accounting for 23.7 percent of all C2 servers found.

Top 5 Most Detected C2 Families	
Family	**2021 C2s**
Cobalt Strike Team Servers	3691
Meterpreter	396
Metasploit	710
QakBot	571
TrickBot	468

Source: Recorded Future

Malicious Infrastructure

2021 Adversary Infrastructure Report

During 2021, Mythic, Covenant, and high-profile use of Silver saw increasing popularity; most other post-exploitation technologies saw comparable levels of deployment as in 2020. Microsoft, RiskIQ, and Insikt Group all discovered cases of initial access brokers establishing ready-to-use Cobalt Strike Team Servers and infections for their clients in 2021. Cobalt Strike C2-as-a-Service was coined to describe this phenomenon.

TrickBot, QakBot, Bazar, IcedID, and Dridex all continued to operate in the absence of Emotet in 2021. IcedID has been related to Egregor deployments, TrickBot and Bazar families have been tied to Ryuk and Conti usage, Dridex has been linked to DoppelPaymer, and QakBot has been linked to ProLock and DoppelPaymer deployments.

While the overall number of C2 servers for Emotet is not as high as for other botnets, Recorded Future believes the infrastructure creation rate shows the operators want to restore Emotet to its former popularity and power.

Recorded Future observed the creation of C2 infrastructure across 130 different countries on 1,650 hosting providers. The data indicates the largest hosting providers are the most abused for C2 hosting; 20 AS operators (12% of total ASNs observed) had more than 100 C2 servers detected on them during 2021. During 2021, 24 of the 130 nations that were seen having C2 servers housed only one C2 server. There were less than 10 C2 servers maintained by 1,454 AS providers (88 percent of total ASNs detected). The top three countries were the United States with the most C2 servers comprising a total of 4,654 servers observed, China was second with 1,949, and coming in third was Germany which had 629 servers.

Digital Ocean, based in the United States, has the highest number of C2s of all of the ASNs tracked by Recorded Future. They were responsible for 968 C2 servers (7.1 percent). With 167 servers, Cobalt Strike was the most often seen family on Digital Ocean. The second largest was the Constant Company (formerly Choopa LLC), a Virtual Private Server provider based in the United States, while Amazon.com Inc., which had the most C2s in 2020, fell to third in 2021.

deepwatch Threat Intel Outlook:

deepwatch Threat Intel Team estimates with moderate confidence that C2 servers will be further insulated and modified in 2022 to prevent discovery. This will most likely result in the removal of traffic from well-known scanning engines and the usage of redirects to hide the Team Server's location (or other C2 nodes). Therefore, to mitigate the risk associated with malicious C2 servers, the Threat Intel Team recommends that customers patch systems and software as soon as possible, have a reliable and tested backup method, and finally, implement multi-factor authentication on exposed remote access systems, such as Remote Desktop, Citirix, and VPN gateways. If possible implementing a Geo-blocking strategy is recommended as data points suggest the C2 IPs are being hosted in countries where organizations do not have business functions such as Russia or Romania.

Ransomware

New Ransomware Spotted: White Rabbit and Its Evasion Tactics

January 18, 2022 Source: *Trend Micro* **Estimated Reading Time:** *2 minutes 45 seconds reading time*

Key Points:

- Trend Micro analyzed a new ransomware family dubbed White Rabbit, with indications that it may be linked to the threat actor FIN8.
- White Rabbit uses a tactic that is also employed by Egregor - password protecting its payload binary. In addition, the links to FIN8 are derived from the use of a URL and a never-before-seen variant of the backdoor Badhatch.
- deepwatch Threat Intel Team judges with **moderate confidence** that the threat actors behind White Rabbit are still developing the ransomware family. In light of this new ransomware family, the best defense is observing malicious activities before the execution of the encryption script. In addition, implement multi-factor authentication on exposed servers, develop an end-user training program, and finally, implement a strong password policy.

Summary:
White Rabbit, a new ransomware family analyzed by Trend Micro, is quietly building a reputation for itself by after launching an attack on a small US bank in December 2021. This newcomer follows in the footsteps of Egregor, a more well-known ransomware family, in concealing its malicious activities. There are indications that it may be linked to the advanced persistent threat (APT) group FIN8.

White Rabbit's payload binary requires a special command-line password to decrypt its internal settings and proceed with its ransomware routine, which is one of the most significant parts of the assault. This way of concealing harmful activities is a strategy used by the Egregor ransomware family to mask malware methods from detection.

Cobalt Strike commands were found in our internal telemetry, which may have been used to reconnoiter, penetrate, and deliver the malicious payload onto the afflicted system. Meanwhile, Lodestone analysts have discovered that the malicious URL linked to the assault is also linked to the APT organization FIN8. They've also pointed out White Rabbit's usage of a never-before-seen variant of Badhatch, an F5 backdoor linked to FIN8. Unfortunately, the files from the specified URL were no longer available at the time of the analysis.

For each file it encrypts, the malware leaves a note. Each note begins with the name of the encrypted file and ends with ".scrypt.txt". Prior to executing the ransomware routine, the malware kills a number of processes and services, particularly those connected to antivirus software. Unless particular files are indicated using the command -f, the malware tries to encrypt data on fixed, removable, and network devices, as well as resources. It also tries to avoid crashing the system and erasing its own notes by skipping specified paths and directories.

Given its simple ransomware routine, Trend Micro believes White Rabbit is still in its early stages of development. Despite its early stage, it is crucial to note that it exhibits the troubling traits of current ransomware: it's extremely targeted and employs double extortion techniques.

deepwatch Threat Intel Outlook:

deepwatch Threat Intel Team judges with **moderate confidence** that the threat actors behind White Rabbit are still developing the ransomware family. At this time more information is needed to conclusively link FIN8 and White Rabbit. But if there is a connection this could indicate how FIN8 is expanding its arsenal to include ransomware, given that they are mostly known for its infiltration and reconnaissance tools. In light of this new ransomware family, the best defense is observing malicious activities before the execution of the encryption script. In addition, implement multi-factor authentication on exposed servers, develop an end-user training program, and finally, implement a strong password policy.

Click here to return to Quick Look

Observables

New Ransomware Spotted: White Rabbit and Its Evasion Tactics

Observables

Description	Value
SHA256	B0844458aaa2eaf3e0d70a5ce41fc2540b7e46bdc402c798dbdfe12b59ab32c3
Trend Micro Signature	Ransom.Win32.WHITERABBIT.YACAET
URL	hxxps://104-168-132-128[.]nip[.]io/cae260

Vulnerability

Mixed Messages: Busting Box's MFA Methods

January 18, 2022 Source: *Varonis* **Estimated Reading Time:** *3 minutes 45 seconds*

Key Points:

- Varonis Threat Labs uncovered a means to overcome multi-factor authentication Box accounts that use an SMS code for login verification.
- A threat actor might use stolen credentials to breach an organization's Box account and exfiltrate sensitive data without having access to the victim's phone if they used this technique.
- deepwatch Threat Intel Team assesses with **moderate confidence** that threat actors are likely to use this technique to access customer networks. Therefore, the Threat Intel Team recommends that customers limit access and monitor the ingress and egress of sensitive data. By doing so, data exfiltration as a result of a perimeter bypass is considerably reduced.

Summary:
For Box accounts that employ an SMS code for login verification, Varonis Threat Labs uncovered a means to overcome multi-factor authentication (MFA). A threat actor might use stolen credentials to breach an organization's Box account and exfiltrate sensitive data without having access to the victim's phone if they used this technique.

Varonis disclosed this issue to Box on November 2, 2021 via HackerOne and Box released a fix.

97,000 businesses, including 68 percent of the Fortune 500, use Box's solutions to access information from anywhere and work with anybody, according to the firm. Users without Single Sign-On (SSO) can utilize an authenticator software like Okta Verify or Google Authenticator, or SMS with a one-time passcode as a second step in authentication, just like many other apps.

Box sets a session cookie and redirects the user to either a form to enter a time-based one-time password (TOTP) if the user is enrolled with an authenticator app, or a form to enter an SMS code if the user enrolled to receive a passcode via SMS after entering a username and password in Box's login form.

The problem arises because even if the user does not navigate to the SMS authentication form, a session cookie is still created. To retrieve a valid session cookie, a threat actor simply has to input the user's email and password—which may be taken through a password breach or phishing attempt, for example. There is no need for an SMS message code.

After generating the cookie, the threat actor can opt out of the SMS-based MFA process (which the user is registered in) and instead employ the TOTP-based MFA process, thus combining MFA modes.

Using the session cookie they got by giving the victim's credentials, the threat actor completes the authentication process by uploading a factor ID and code from their own Box account and authenticator app to the TOTP verification endpoint.

Box does not confirm the victim was registered for TOTP verification or that the authenticator app being used belongs to the user who was logging in. This allowed the threat actor to gain access to the victim's Box account without using the victim's phone or sending an SMS notification.

Varonis has provided a video of the attack in action here.

Vulnerability

Mixed Messages: Busting Box's MFA Methods

Attack Flow

1. The threat actor uses an authenticator app to enroll in multi-factor authentication and saves the device's factor ID.
2. On account.box.com/login, the threat actor enters a user's email address and password.
3. If the password is correct, a new authentication cookie is given to the attacker's browser, which redirects to /2fa/verification.
4. However, the attacker ignores the link to the SMS verification form. Instead, users use the authenticator app to input their own factor ID and code to the TOTP verification form at /mfa/verification.
5. The threat actor has gained access to the victim's account, and the victim is no longer receiving SMS messages.

Varonis revealed not one, but two application issues that allowed us to log into a victim's MFA-enabled Box account using just their username and password. Unfortunately, Box isn't the only large SaaS company Varonis was able to bypass.

Varonis recommends that organization CISOs ask themselves the following questions:

- Would I be able to tell if a user's MFA has been disabled or circumvented across all of my SaaS applications?
- How much information can a threat actor have access to if they gain control of a regular user account?
- Is there any data that is unnecessarily shared with a large number of people (or that is shared publicly)?
- Will I be notified if a user accesses data in an unusual way?

deepwatch Threat Intel Outlook:

deepwatch Threat Intel Team assesses with **moderate confidence** that threat actors are likely to use this technique to access customer networks. Therefore, the Threat Intel Team recommends limiting access to sensitive data and monitoring the ingress and egress of sensitive data. By doing so data exfiltration as a result of a perimeter bypass is considerably reduced.

deepwatch

Exploited Vulnerabilities

CISA Adds 13 Known Exploited Vulnerabilities to Catalog

January 18, 2022 Source: *CISA* **Estimated Reading Time:** *1 minute*

Key Points:

- CISA has added 13 new vulnerabilities to its Known Exploited Vulnerabilities Catalog.
- Threat actors are actively exploiting these vulnerabilities, which are common attack vectors.
- deepwatch Threat Intel Team strongly urges all customers to prioritize timely remediation of vulnerabilities featured in CISAs Known Exploited Vulnerabilities Catalog as part of their vulnerability management practice.

Summary:
Based on evidence that threat actors are exploiting the 13 vulnerabilities listed in the table below, CISA has added them to its Known Exploited Vulnerabilities Catalog. CISA strongly advises all organizations to prioritize quick remediation of the vulnerabilities listed in the Known Exploited Vulnerabilities Catalog as part of their vulnerability management strategy to decrease their exposure to attacks.

CVE	Description
CVE-2021-32648	October CMS Improper Authentication
CVE-2021-21315	System Information Library for node.js Command Injection Vulnerability
CVE-2021-21975	Server Side Request Forgery in vRealize Operations Manager API Vulnerability
CVE-2021-22991	BIG-IP Traffic Microkernel Buffer Overflow Vulnerability
CVE-2021-25296	Nagios XI OS Command Injection Vulnerability
CVE-2021-25297	Nagios XI OS Command Injection Vulnerability
CVE-2021-25298	Nagios XI OS Command Injection Vulnerability
CVE-2021-33766	Microsoft Exchange Server Information Disclosure Vulnerability
CVE-2021-40870	Aviatrix Controller Unrestricted Upload of File Vulnerability
CVE-2020-11978	Apache Airflow Command Injection Vulnerability
CVE-2020-13671	Drupal Core Unrestricted Upload of File Vulnerability
CVE-2020-13927	Apache Airflow Experimental API Authentication Bypass Vulnerability
CVE-2020-14864	Oracle Corporate Business Intelligence Enterprise Edition Path Traversal Vulnerability

deepwatch Threat Intel Outlook:

deepwatch Threat Intel Team strongly urges all customers to prioritize rapid remediation of vulnerabilities listed in CISA's Known Exploited Vulnerabilities Catalog as part of their vulnerability management process. In addition, the Threat Intel Team at deepwatch will continue to monitor new vulnerabilities added to the Catalog and keep customers informed via the weekly Cyber Intel Brief.

Click here to return to Quick Look

Best Practices

Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats

January 18, 2022 Source: *CISA* **Estimated Reading Time:** *2 minutes*

Key Points:

- CISA published "CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats" in response to the recent malicious cyber incidents in Ukraine.
- In the CISA insights they layout steps and guidance for organizations to aid in reducing the likelihood of a damaging cyber intrusion, steps to quickly detect a potential intrusion, steps to ensure that organizations are prepared to respond if an intrusion occurs, and finally, how to maximize resilience to a destructive cyber incident.
- deepwatch Threat Intel Team highly encourages all customers to follow CISAs guidance to make immediate progress toward enhancing cybersecurity and resilience by following the actions outlined in the CISA Insights. Furthermore, the Threat Intel Team recommends customers reference CIB-21-02 for a summary on "Understanding and Mitigating Russian State-Sponsored Cyber Threats to US Critical Infrastructure."

Summary:

"CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats" (*PDF*) was issued in reaction to recent malicious cyber incidents in Ukraine, including the defacement of official websites and the presence of potentially dangerous malware on Ukrainian systems. The CISA Insights strongly advises leaders and network defenders to be on the lookout for hostile cyber activity and gives a checklist of tangible steps that any company, regardless of sector or size, may do right away to:

- Reduce the chances of a devastating cyber-attack.
- Detect a possible incursion, ensure the business is prepared to respond if one happens, and increase the organization's resilience to a damaging cyber event.
- Senior executives and network defenders should read the CISA Insights and put the cybersecurity measures on the checklist into action, according to CISA.

In the CISA insights they layout steps and guidance for organizations to aid in reducing the likelihood of a damaging cyber intrusion, steps to quickly detect a potential intrusion, steps to ensure that organizations are prepared to respond if an intrusion occurs, and finally, maximize resilience to a destructive cyber incident.

deepwatch Threat Intel Outlook:

deepwatch Threat Intel Team highly encourages all customers to follow CISAs guidance to make immediate progress toward enhancing cybersecurity and resilience by following the actions outlined in the CISA Insights. Furthermore, while recent cyber events have yet to be linked to specific actors, the Threat Intel Team recommends customers reference CIB-21-02 for a summary on "Understanding and Mitigating Russian State-Sponsored Cyber Threats to US Critical Infrastructure." It is also recommended by CISA that customers visit StopRansomware.gov, a consolidated, whole-of-government website with ransomware tools and warnings.

Appendices & Feedback

Appendix A

Purpose

This report is provided to you to improve your situational awareness and educate recipients on the latest cyber threats to aid customers' in protecting the confidentiality, integrity, and access of their organizations' networks and assets. In addition, deepwatch includes an intelligence assessment and recommendations to mitigate the risk.

Sources of Information

This publication incorporates open-source news articles to educate readers on cybersecurity matters IAW USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement.

Use and Definitions

To help you use this document to its full potential, a few items may be helpful to know:

- You can click on any headline in the table of contents to take you to that portion of the report.
- Links throughout this document are identified by the font color of "deepwatch" green.
- Each headline will be categorized; these categories quickly let you know what the main topic of the headline is.
- **Each headline this report covers includes the following information:**
    - Publication date, link to the source material, and estimated reading time.
    - Key Points section to get the most important information first.
    - Summary - This is a brief synopsis of the reporting to bring you only the most relevant information. If applicable, deepwatch will link items of interest for further context; these will be denoted in "deepwatch" green.
    - deepwatch Threat Intel Outlook: - This section includes the Threat Intel Teams assessment of the likelihood that the activity will continue in the near future. In addition, additional analysis and reporting on the activity, recommendations, and any actions deepwatch may have taken with the available information may be included.

Click here to return to Table of Contents

Appendix B

What We Mean When We Say: An Explanation of Estimative Language

To convey analytical assessments and judgments, the Threat Intel Team uses phrases like judge, assess, and estimate, as well as probabilistic terms like probably and likely. Such claims are not based on facts, proof, or knowledge. These evaluations and judgments are frequently based on gathered data that is often incomplete or fragmentary. Some evaluations are based on prior judgments. In all cases, assessments and judgments are not meant to imply that we have "proof" that something is a fact or that two items or issues are inextricably linked.

in addition to conveying judgments rather than certainty, our estimative language frequently conveys 1) our assessed likelihood or probability of an event; and 2) the level of confidence we attribute to the judgment.

Estimates of Likelihood. We use probabilistic language to reflect the Intel Team's estimates of the likelihood of developments or events because analytical judgments are not certain. Terms like "probably," "likely," "very likely," and "almost certainly" denote a higher than even chance. The terms unlikely and remote imply that an event has a lower than even chance of occurring; they do not imply that it will not. Terms like might and might reflect situations where we are unable to assess the likelihood, usually due to a lack of relevant information, which is sketchy or fragmented. Terms like "we can't dismiss," "we can't rule out," and "we can't discount" refer to an unlikely, improbable, or distant event with significant consequences.

Confidence in Assessments. Our assessments and projections are based on data that varies in scope, quality, and source. As a result, we assign our assessments high, moderate, or low levels of confidence, as follows:

- High confidence indicates that our decisions are based on reliable information and/or that the nature of the problem allows us to make a sound decision. However, a "high confidence" judgment is not a fact or a guarantee, and it still carries the risk of being incorrect.
- Moderate confidence denotes that the information is credible and plausible, but not of high enough quality or sufficiently corroborated to warrant a higher level of assurance.
- Low confidence indicates that the information's credibility and/or plausibility are in doubt, that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that we have serious concerns or problems with the sources.

Feedback

Please take a few minutes to send us your feedback by filling out the form below and emailing it to dw-threat-operations@deepwatch.com or submitting it here. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the deepwatch Threat Intel Team. Feedback should be specific to your experience with this written product to enable deepwatch to make quick and continuous improvements to these products.

First Name (optional) _____

Last Name (optional) _____

Which category best describes your job title? *

How would you rate this product overall? *

The information provided was relevant and useful? *

The information provided was timely for the appropriate action? *

What are your thoughts on the length of the document? *

How likely are you to share this product with an associate or colleague? *

What was most helpful about the information? (optional)

What was the least helpful about the information? (optional)

Please provide suggestions or any other overall comments as to how our reporting can be improved. (optional)

