Hades Ransomware Operators Use Distinctive Tactics and Infrastructure

Commonalities revealed during multiple Secureworks incident response engagements provided insights into the GOLD WINTER threat group's tactics, techniques, and procedures.

TUESDAY, JUNE 15, 2021BY: COUNTER THREAT UNIT RESEARCH TEAM

Hades ransomware has been on the scene since December 2020, but there has been limited public reporting on the threat group that operates it. Secureworks® incident response (IR) engagements in the first quarter of 2021 provided Secureworks Counter Threat Unit™ (CTU) researchers with unique insight into the group's use of distinctive tactics, techniques, and procedures (TTPs).

The financially motivated threat group operating the Hades ransomware is known as GOLD WINTER. Some third-party reporting attributes Hades to the HAFNIUM threat group, but CTU™ research does not support that attribution. Other reporting attributes Hades to the financially motivated GOLD DRAKE threat group based on similarities to that group's WastedLocker ransomware. Despite use of similar application programming interface (API) calls, the CryptOne crypter, and some of the same commands, CTU researchers attribute Hades and WastedLocker to two distinct groups as of this publication.

Ransomware groups are typically opportunistic: they target any organization that could be susceptible to extortion and will likely pay the ransom. However, GOLD WINTER's attacks on large North America-based manufacturers indicates that the group is a "big game hunter" that specifically seeks high-value targets.

Unique TTPs

Analysis of these IR engagements revealed TTPs not associated with other ransomware families. Some of the tactics and tools may be similar to those used by other threat groups, but GOLD WINTER added some unusual aspects.

'Tox'-ic conversations

Hades' absence on underground forums and marketplaces suggests that it is operated as private ransomware rather than ransomware as a service (RaaS). GOLD WINTER "names and shames" victims after stealing their data but does not use a centralized leak site to expose the exfiltrated data. Instead, Tor-based Hades websites appear to be customized for each victim (see Figure 1). Each website includes a victim-specific Tox chat ID for communications (see Figure 1). Using Tox instant messaging for communications is a novel technique that CTU researchers have not observed with other ransomware families.

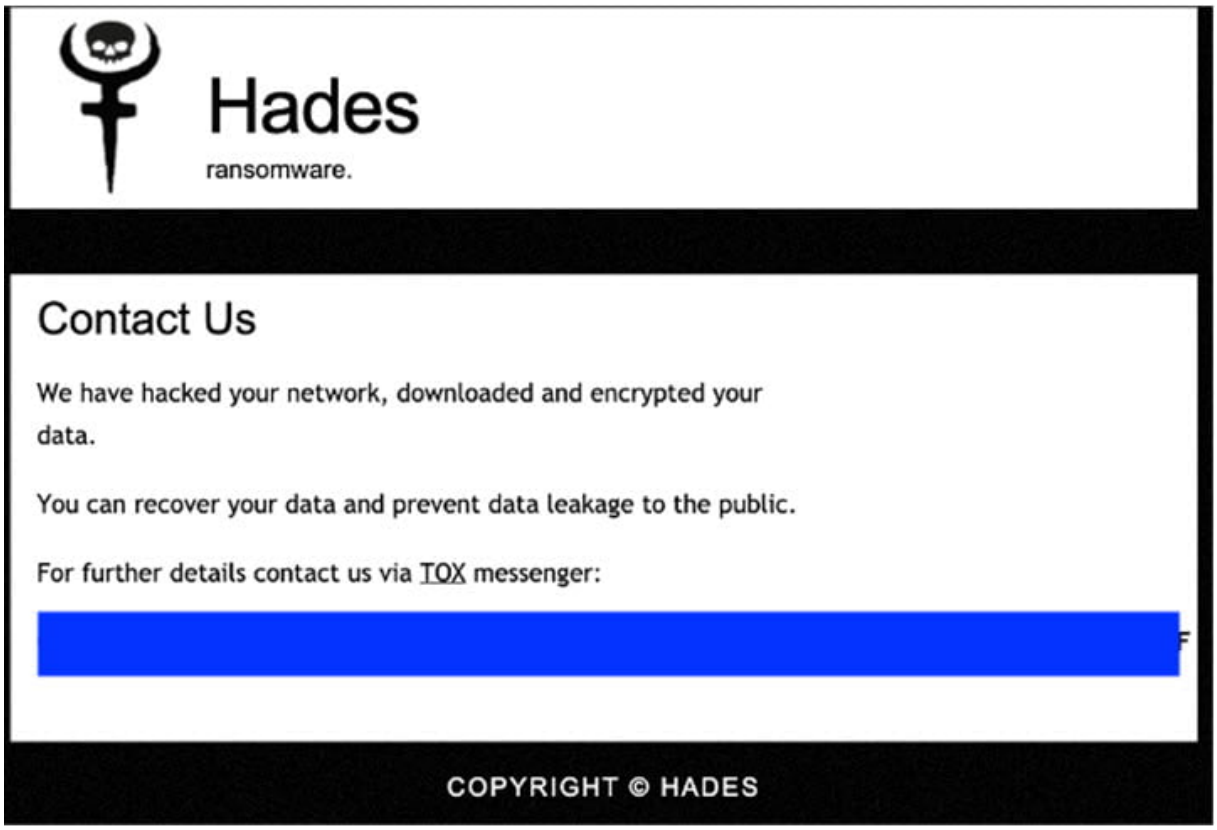
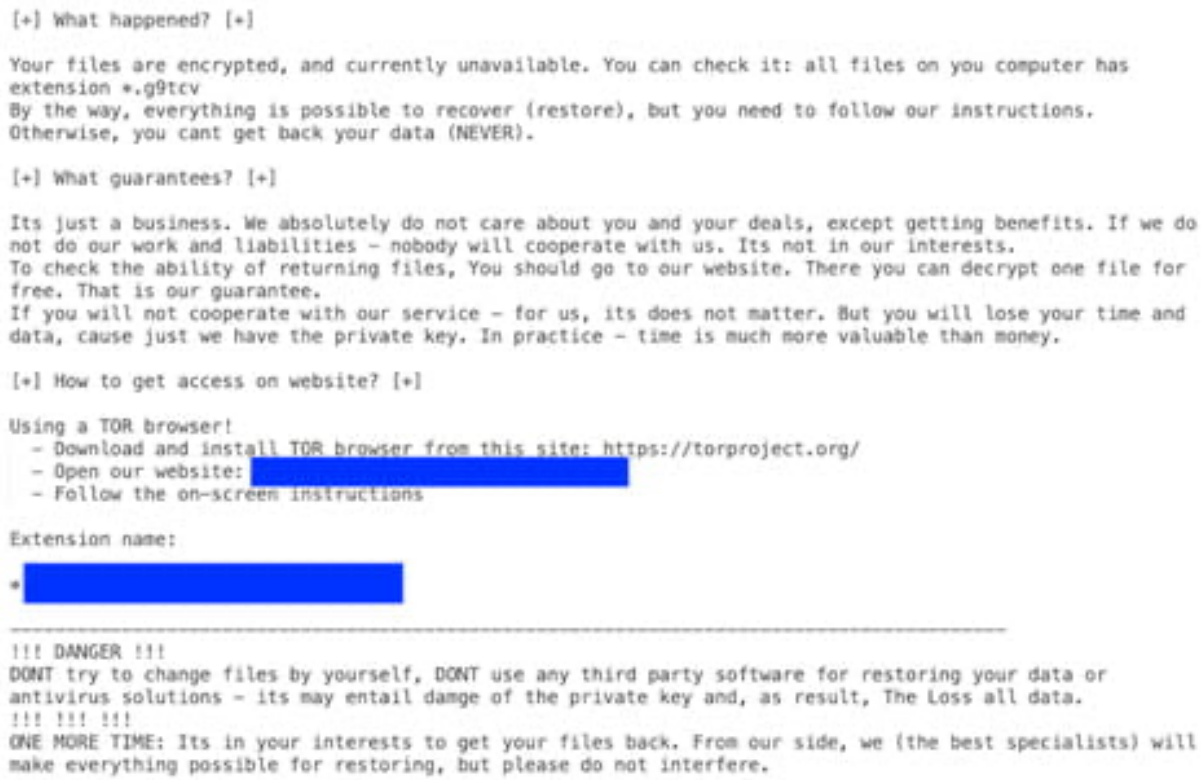


Figure 1. Hades ransomware victim site. (Source: Secureworks)

Imitation is the sincerest form of flattery

GOLD WINTER has a propensity for copying ransom notes from other high-profile ransomware families. The Hades ransom note samples observed by CTU researchers duplicated REvil or Conti ransom notes. The REvil look-alike ransom note (HOW-TO-DECRYPT-<*victim ID*>.txt) featured a unique victim identifier that was hard-coded in the ransomware executable (see

Figure 2). This ransom note referred each victim to a personalized Tor victim site, whose URL is hard-coded in the malware.



```
[+] What happened? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has
extension *.g9tcv
By the way, everything is possible to recover (restore), but you need to follow our instructions.
Otherwise, you cant get back your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do
not do our work and liabilities - nobody will cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for
free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and
data, cause just we have the private key. In practice - time is much more valuable than money.

[+] How to get access on website? [+]

Using a TOR browser!
  - Download and install TOR browser from this site: https://torproject.org/
  - Open our website: [redacted]
  - Follow the on-screen instructions

Extension name:

*[redacted]

--------------------------------------------------------------------------------

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or
antivirus solutions - its may entail damge of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) will
make everything possible for restoring, but please do not interfere.
```

Figure 2. REvil look-alike ransom note used by GOLD WINTER. (Source: Secureworks)

In early April, CTU researchers observed the threat actors dropping a Conti look-alike ransom note (CONTACT-TO-DECRYPT.txt). It included contact email addresses instead of a website, indicating a potential change in TTPs. GOLD WINTER may use look-alike ransom notes to confuse researchers or perhaps to pay homage to admired ransomware families.

Name game

CTU researchers also observed the threat actors shifting from using a randomly generated five-character string for the victim ID and encrypted file extension to using words. A March IR engagement revealed use of a single word: “cypherpunk”. Based on the definition of this term, perhaps the threat actors view their ransomware activity as a way to prompt organizations to improve their security.

Two IAVs are better than one

CTU researchers identified two distinct initial access vectors (IAVs) across the analyzed environments. In some intrusions, the threat actors used stolen or guessed credentials to log in via a virtual private network (VPN) that did not implement multi-factor authentication. The second IAV was SocGholish malware delivered via fake browser updates. SocGholish is commonly associated with the GOLD DRAKE threat group.

Threat actor toolbox

GOLD WINTER's tools include Cobalt Strike Malleable C2, Mimikatz, Advanced Port Scanner, PsExec, Metasploit, and MSBuild. Most of these tools are commonly observed in compromised environments. But in one uncommon implementation used in a Hades intrusion, MSBuild executed a file containing a Metasploit payload (see Figure 3).

```
cmd /c
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.
exe C:/ProgramData/ytuf.proj
```

Figure 3. MSBuild used to execute malicious file. (Source: Secureworks)

CTU researchers also observed two scripts that repeatedly stopped services (see Figure 4) and cleared event logs (see Figure 5). Both scripts featured a distinctive 60-second 'sleep' loop.

```
:start
wmic service where "caption like '%%SQL%%'" call stopservice
wmic service where "caption like '%%Microsoft Exchange%%'" call stopservice
wmic product where name="Microsoft Security Client" call uninstall /
nointeractive
reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SepMasterService" /v
Start /t REG_DWORD /d 4 /f
taskkill /f /im ccSvcHst.exe
timeout 60
goto start
```

Figure 4. Batch script to stop services. (Source: Secureworks)

```
:start
for /F "tokens=*" %%1 in ('wevtutil.exe el') DO wevtutil.exe cl "%%1"
timeout 60
goto start
```

Figure 5. Batch script to clear event logs. (Source: Secureworks)

The threat actors disguised the Cobalt Strike executable as a Corel Draw graphics application (see Figure 6) to obfuscate the true nature of the file. While spoofing legitimate applications is not unusual, the use of Corel Draw is unique.

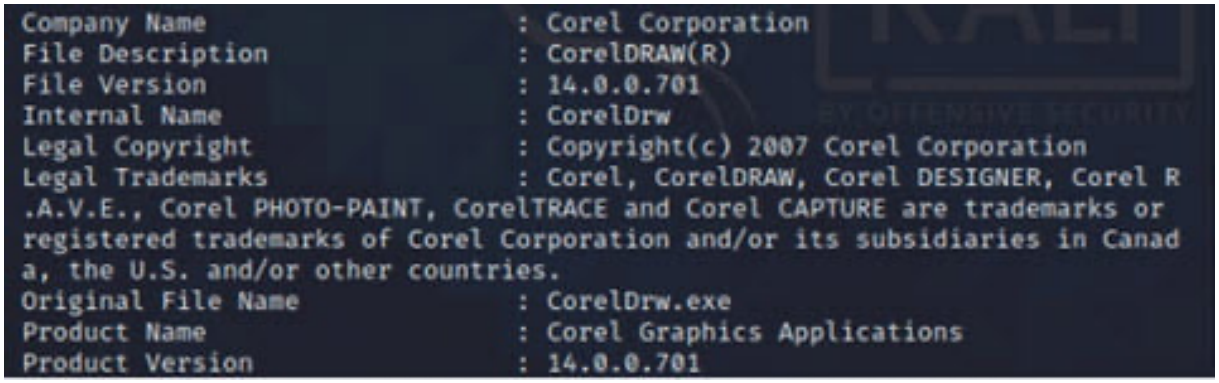


Figure 6. EXIF data associated with Cobalt Strike disguised as Corel Draw. (Source: Secureworks)

GOLD WINTER has used Remote Desktop Protocol (RDP) and reverse SOCKS proxies (see Figure 7) to maintain access to victims' environments. The MEGAsync cloud storage platform was used for data exfiltration.

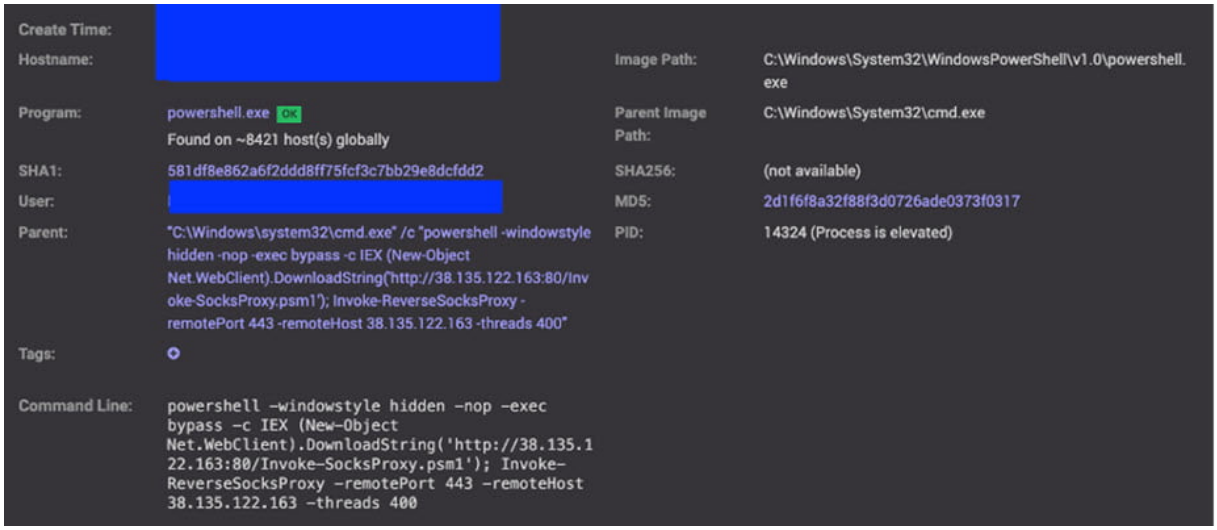


Figure 7. Reverse SOCKS proxy invocation. (Source: Secureworks)

Ransomware analysis

Some Hades samples analyzed by CTU researchers use the "ClassicStartMenu.exe" filename and have December 2020 creation dates,

which coincides with the first reports of the ransomware. The Hades ransomware executable copies itself into a random %AppData% folder and then executes via the “/go” argument. It checks the compromised environment for virtualization and debugging tools. Like many other ransomware families, Hades deletes volume shadow copies using the “vssadmin.exe Delete Shadows /All /Quiet” command. It also uses a distinctive self-delete command with an unusual inclusion of a waitfor command: cmd /c waitfor /t 10 pause /d y & del "*<ransomware file path>*" & rd "*<ransomware folder>*".

Infrastructure

CTU researchers observed commonalities across IP addresses and domains used by GOLD WINTER. The threat actors leveraged IP provider Selectel (see Figure 8), and the IP addresses fall under AS49505.

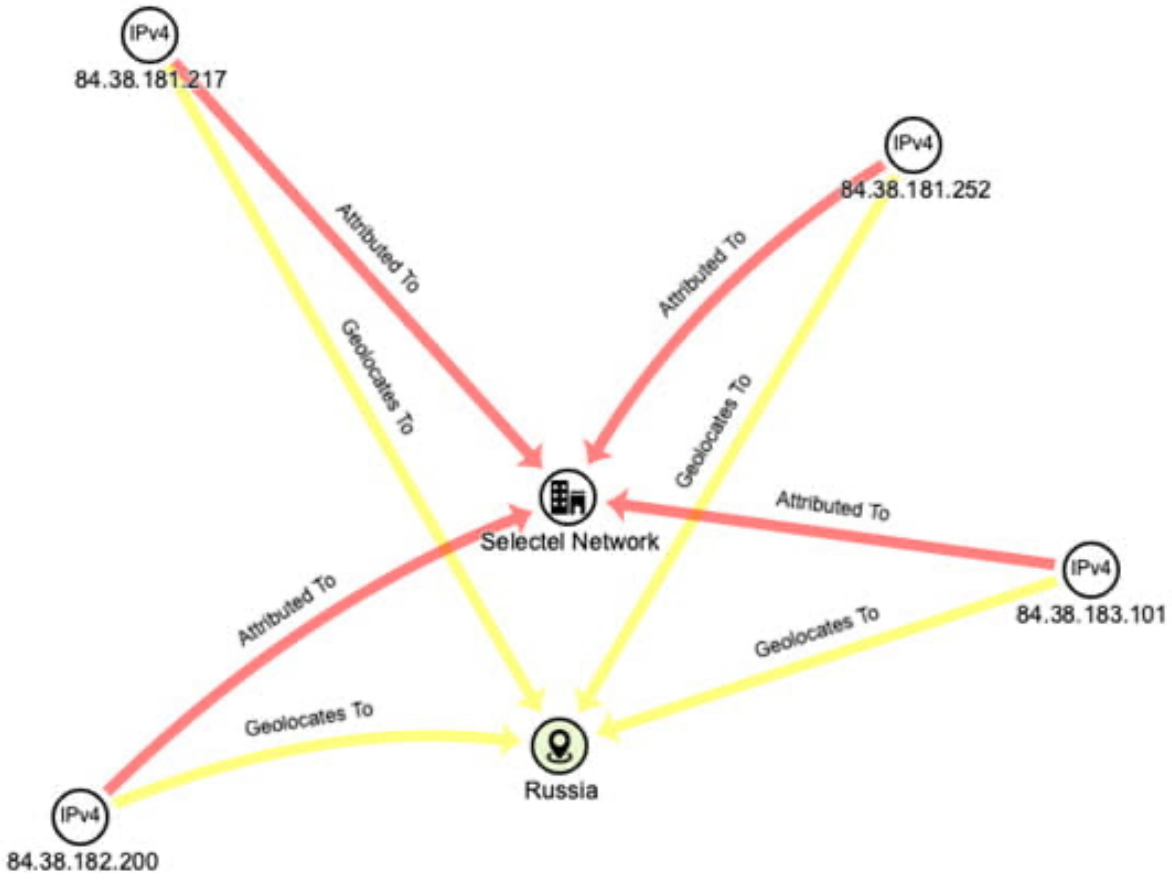


Figure 8. IP addresses used by GOLD WINTER. (Source: Secureworks)

The domains associated with GOLD WINTER infrastructure were issued by Russian registrar REG.RU (see Figure 9). Most of these domains were

created in June 2020; the exception is bingoshow . xyz, which was registered in January 2021. Registration data for this domain shows the state as Indiana but a country code for Finland and a New Jersey phone number, likely indicating that the threat actors deliberately provided misinformation. All the identified domains have links to the identified Selectel IP addresses.

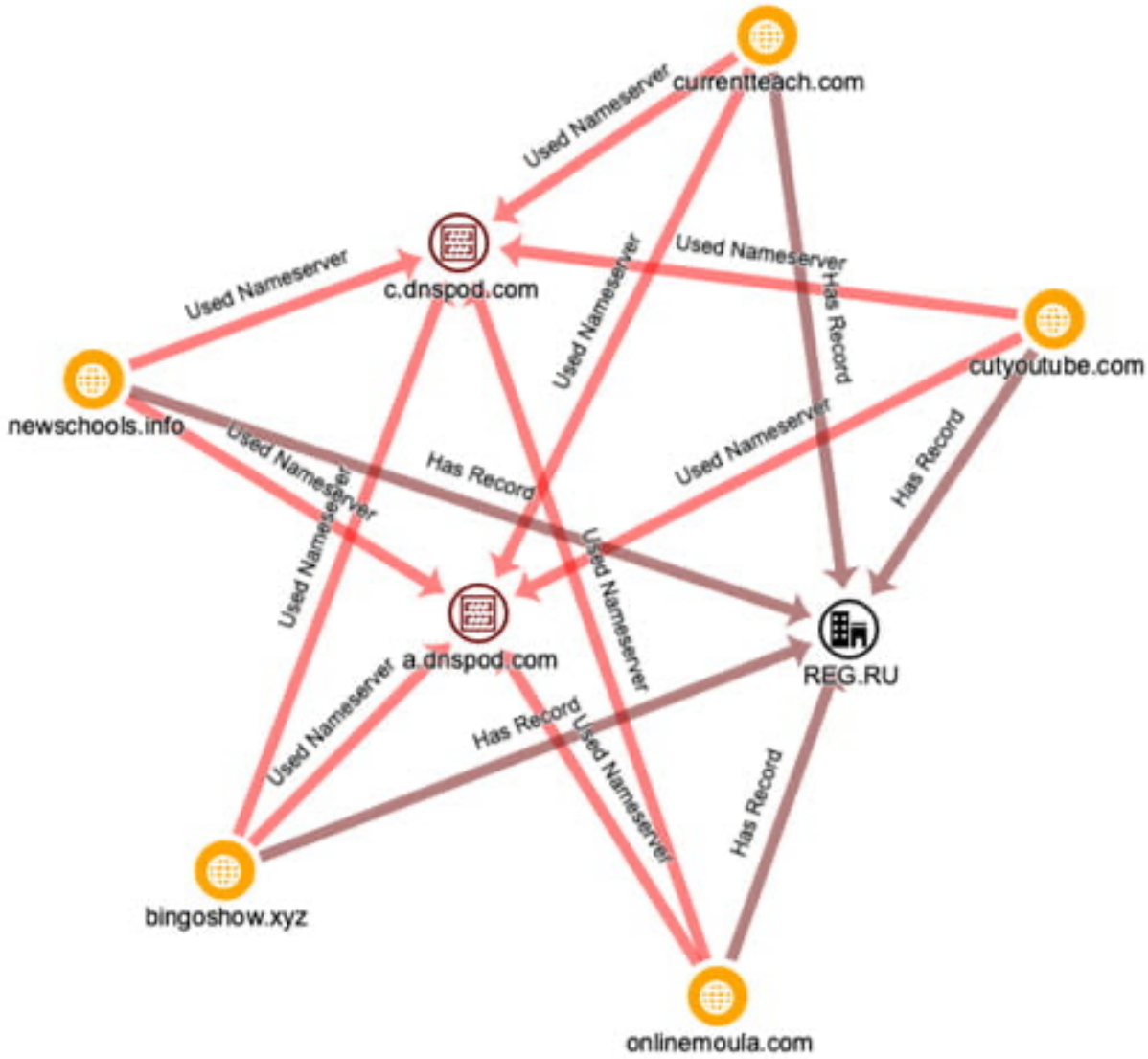


Figure 9. Domains used by GOLD WINTER. (Source: Secureworks)

Conclusion

CTU researchers track threats and behaviors identified during IR engagements to understand the nature and evolution of various threats. Through countermeasure development, periodic trend analysis, and ad-hoc tactical reporting on activity observed during these engagements, CTU

researchers continuously provide protection, insight, and guidance derived from real-world incidents to Secureworks customers. In many ways, the GOLD WINTER threat group is a typical post-intrusion ransomware threat group that pursues high-value targets to maximize how much money it can extort from its victims. However, GOLD WINTER's operations have quirks that distinguish it from other groups.

It is crucial for organizations to diligently respond to early signs of threat actor activity before encryption occurs. Staying one step ahead of the threat actors is increasingly difficult as they evolve their TTPs. Organizations do not have the luxury of time when it comes to investigating pre-infection activity.

Learn more about Secureworks proactive and reactive IR services, including process evaluations, training exercises, emergency response, and IR retainers.

Threat Indicators

To mitigate exposure to this threat, CTU researchers recommend that organizations use available controls to review and possibly restrict access using the indicators in Table 1. Note that IP addresses can be reallocated. The IP addresses and domains may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
cutyoutube.com	Domain name	Cobalt Strike C2 server used in Hades ransomware attacks
onlinemoula.com	Domain name	Cobalt Strike C2 server used in Hades ransomware attacks
bingoshow.xyz	Domain name	Hades ransomware victim site
bingoshowxyz.com	Domain name	Hades ransomware victim site
ddb4a151.news.pocketstay.com	Domain name	SocGholish C2 server used in Hades ransomware attacks
5lyi3c7x3ioakru4.onion	Domain name	Hades ransomware Tor victim site
o76s3m7l5ogig4u5.onion	Domain name	Hades ransomware Tor victim site
92726558efc81ee1ace4036b43fa003b	MD5 hash	Cobalt Strike disguised as Corel Draw in Hades ransomware attacks
509833d7724f49a03dadd5668610d464593322b7	SHA1 hash	Cobalt Strike disguised as Corel Draw in Hades ransomware attacks

Indicator	Type	Context
d7e3342f316d783e4ae6447837173bfe060aaaef37553b9d67719653213bc868	SHA256 hash	Cobalt Strike disguised as Corel Draw in Hades ransomware attacks
d9eed5c4fa18ee594f7d3edf5d0ce5bf	MD5 hash	SocGholish disguised as fake Chrome update in Hades ransomware attacks
5455f9e07d45f3f9cca6eadc95b75858cda7ee87	SHA1 hash	SocGholish disguised as fake Chrome update in Hades ransomware attacks
6a7f477dcf96c2b648a3de66ea331e984305a4bc80571282b183713ae82613a2	SHA256 hash	SocGholish disguised as fake Chrome update in Hades ransomware attacks
7a0a3e5189f78565b48c36ca226f223a	MD5 hash	Hades ransomware
e8d485259e64fd375e03844c03775eda40862e1c	SHA1 hash	Hades ransomware
1526fc970cdb0e5a69f0ca2284d12312c6f7c9d0e77aa264aa4260411a4f03e7	SHA256 hash	Hades ransomware
cf3e421ab7f5ce169d12d24873c30e84	MD5 hash	Hades ransomware
d2e5fa5510484e99041ed8a4f16acfa40f7a78f6	SHA1 hash	Hades ransomware
90dfa6dfd55f6db1f79016f69047265e2a3cb42d9e7a74a5142918c04a3b1cec	SHA256 hash	Hades ransomware
84.38.183.101	IP address	Used in Hades ransomware attacks
84.38.181.252	IP address	Hosting Hades ransomware victim site
84.38.181.217	IP address	Cobalt Strike C2 server used in Hades ransomware attacks
84.38.182.200	IP address	Cobalt Strike C2 server used in Hades ransomware attacks
79.110.52.138	IP address	SocGholish fake Chrome update C2 server used in Hades ransomware attacks
130.0.233.178	IP address	SocGholish fake Chrome update C2 server used in Hades ransomware attacks
165.225.116.28	IP address	Cobalt Strike C2 server used in Hades ransomware attacks
38.135.122.163	IP address	Reverse SOCKS proxy used in Hades ransomware attacks
80.92.205.205	IP address	Used in Hades ransomware attacks

Table 1. Indicators for this threat.