Threat Attribution — Chimera “Under the Radar”

cycrafttechnology.medium.com/threat-attribution-chimera-under-the-radar-7c4cce390efd

CyCraft Technology Corp May 19, 2021

CyCraft Technology Corp

Jan 26, 2021

.

8 min read

CYCRAFT
THREAT ATTRIBUTION :
CHIMERA "UNDER THE RADAR"
THREAT ATTRIBUTION RESEARCH COMPARISON

Threat Attribution Research Comparison

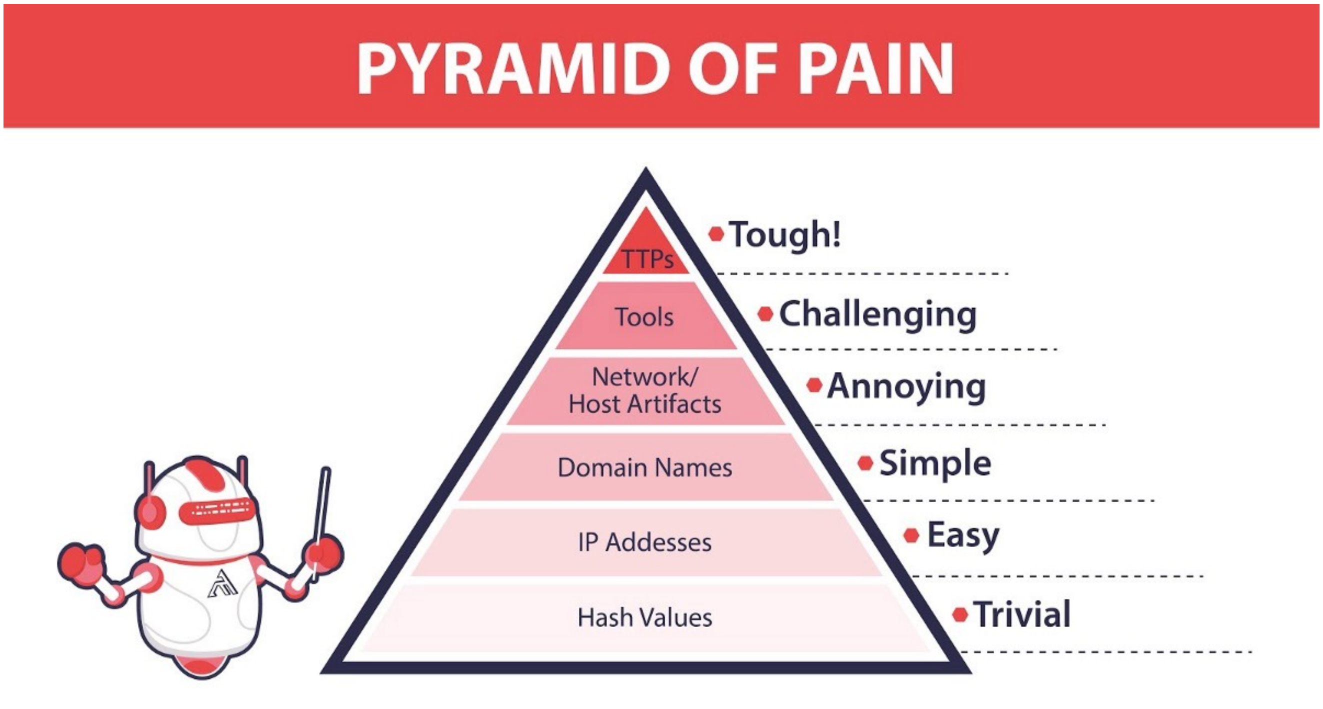
On 12 January 2021, Fox-IT & NCC Group published their detailed report, “Abusing Cloud Services to Fly Under the Radar”. The threat actor tracked in their report shared many similarities to the China-linked threat actor Chimera, whom CyCraft attributed to a year-long cyberattack targeting the Taiwan semiconductor industry just last year.

Much like Chimera, the threat actor mentioned in the Fox-IT & NCC Group report (referred to in this article as CUTR, Chimera Under the Radar) targeted intellectual property (IP) from the semiconductor industry; however, the report goes into further detail explaining how their threat actor’s targets were more diverse, including targeting sensitive data from the EU aviation industry.

In this article, we analyze and compare their research to ours.

Conclusions

1. There is a strong probability the threat actor, CUTR, is Chimera as their IoCs, commonly used infra, tools, techniques, and behaviors are all very similar to Chimera; 42 of the 67 adversarial techniques used in both campaigns were identical.
2. China-linked threat actors (e.g., Chimera, BlackTech, APT30) are known to share tools and attack methods with each other, making attribution challenging.
3. Some differences in attack behavior may be due to differences in the victims’ architecture, security maturity, or geographic location (EU, not Taiwan). Different environments may require different TTP. TTP designed for infiltrating Taiwan’s semiconductor industry may require adjustment for the EU aviation industry and vice versa.
4. Chimera was focused solely on the Taiwan semiconductor industry. CUTR showed “a wide set of interests,” including the EU semiconductor industry as well as aviation. While some China-linked threat actors have demonstrated an ability to adapt techniques, tools, and targets, sudden changes in attack behavior are not common — keeping true to the ideas behind Bianco’s Pyramid of Pain, as mentioned in the Fox-IT & NCC Group report. As TTPs are the hardest to change and tend to stay inflexible for longer periods of time, similar TTP usage between different attack campaigns/operations is a strong indicator of attribution.



As mentioned in the FOX-IT & NCC Group report, Bianco's Pyramid of Pain illustrates how difficult it is for an attacker to circumvent a particular attack method that has been stripped away from them. For example, while blocking a file or IP address is rather trivial for an attacker to get around, taking away an attacker's tool is challenging; they will have to devise a new way of carrying out their objectives.

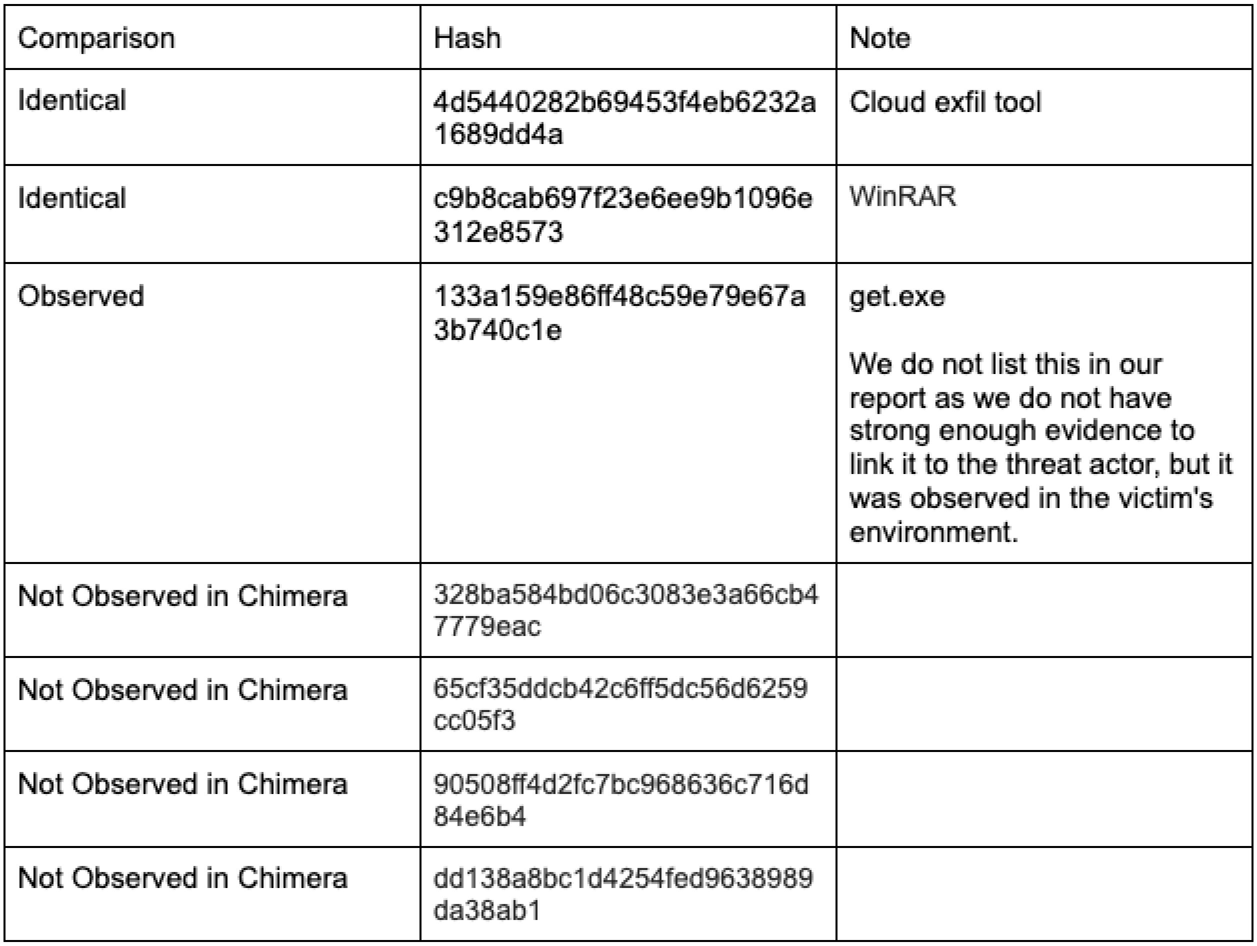
According to the Fox-IT & NCC Group report, "the largest overlap [between Chimera and their threat actor] is in the top half of the Pyramid of Pain: domain names, host artifacts, tools, and TTPs."

We will compare Chimera with CUTR using the Pyramid of Pain model from the ground up.

Hash Values

The following table shows the hash of these IoCs. As depicted in the table, 3 of the hashes are identical to our research. Even though the identical WinRAR and get.exe can be easily used by other threat actors, the added inclusion of the Cloud exfil tool increases the probability of Chimera attribution.

Chimera primarily used both the Cobalt Strike Beacon and the Winnti backdoors during their operation against Taiwan's semiconductor industry. CUTR was not observed using the Winnti backdoor but was observed using Cobalt Strike Beacon's remote access functionality; however, we cannot confirm if it is the exact same Cobalt Strike Beacon as Fox-IT & NCC Group did not release the hash in their report.



Comparison	Hash	Note
Identical	4d5440282b69453f4eb6232a1689dd4a	Cloud exfil tool
Identical	c9b8cab697f23e6ee9b1096e312e8573	WinRAR
Observed	133a159e86ff48c59e79e67a3b740c1e	get.exe We do not list this in our report as we do not have strong enough evidence to link it to the threat actor, but it was observed in the victim's environment.
Not Observed in Chimera	328ba584bd06c3083e3a66cb47779eac	
Not Observed in Chimera	65cf35ddcb42c6ff5dc56d6259cc05f3	
Not Observed in Chimera	90508ff4d2fc7bc968636c716d84e6b4	
Not Observed in Chimera	dd138a8bc1d4254fed9638989da38ab1	

```
4d5440282b69453f4eb6232a1689dd4ac9b8cab697f23e6ee9b1096e312e8573133a159e86ff48c59e79e6
```

IP address & Domain Name

None of the domain names are identical, but the behavior of abusing the cloud platforms such as Appspot or Azure Edge is aligned with our findings. This increases the probability of Chimera attribution.

Network & Host Artifacts

Some file names used are similar to our research. Here we list some similar naming schemes.

> RecordedTV.ms
> OneDrive.exe
> update.exe
> jucheck.exe

Tool

The tools used by their threat actor significantly overlap with our research into Chimera.

> Cobalt Strike
> OneDrive
> Modified RAR
> Cloud Service

TTP

According to the Pyramid of Pain model, TTP are the most difficult and less frequently changed methods of an attacker, suggesting that campaigns/operations with multiple similarities in TTP are most likely performed by the same threat actor.

Comparing the adversarial techniques used by Chimera and CUTR, 42 of the 67 adversarial techniques used in both campaigns were identical. Below are a few notable similarities and differences.

Techniques critical to both Chimera & CUTR's attack behavior:

> T1003.003 OS Credential Dumping: NTDS
> T1003.001 OS Credential Dumping: LSASS Memory
> T1053.005 Scheduled Task/Job: Scheduled Task
> T1078 Valid Accounts

Observed only in CUTR:

> T1574.002 Hijack Execution Flow: DLL Side-Loading
> T1111 Two-Factor Authentication Interception
> T1550.002 Use Alternate Authentication Material: Pass the Hash

Observed only in Chimera:

> T1055.001 Process Injection: Dynamic-link Library Injection
> T1556.001 Modify Authentication Process: Domain Controller Authentication

Differences in attack behavior may be due to differences in the victims' architecture, security maturity, geographic location (EU, not Taiwan), or differences in visibility.

Both threat actors are China-based and located in the UTC +8 timezone.

The TTP used by both Chimera and CUTR are summarized below — mapped in the MITRE ATT&CK® framework.

Initial Access

Execution

Credential Access

Lateral Movement

Collection

Exfiltration

Summary

Threat attribution is difficult.

China-linked threat actors are known to share tools and attack methods (and possibly even personnel) with each other. Differences in victim security operational culture, geographic location, system architecture, security maturity, industry, and defense technology can all lead to minor and major differences in attack behavior. There are always numerous factors to consider and weigh, making perfect attribution difficult.

However, the evidence presented after comparing research from both CyCraft and Fox-IT & NCC Group illustrates a strong likelihood that CUTR is Chimera.

Chimera and CUTR are both located in the UTC +8 timezone, are China-based, and have a strong overlap in IoCs, commonly used infra, tools, techniques, and behavior. 42 of the 67 adversarial techniques used in both Chimera and CUTR campaigns were identical.

CyCraft confirms with high confidence that CUTR is Chimera.

We would like to thank Fox-IT & NCC Group for their detailed report, added visibility into the Chimera threat, and added threat intelligence against this China-based threat actor so that SOCs can better defend their organizations and keep their data secure.

Everything Starts From Security

CyCraft Customers can prevent cyber intrusions from escalating into business-altering incidents. From endpoint to network, from investigation to blocking, from in-house to cloud, CyCraft AIR covers all aspects required to provide small, medium, and large organizations with the proactive, intelligent, and adaptable security solutions needed to defend from all manner of modern security threats with real-time protection and visibility across the organization.

Engage with CyCraft

engage@cycraft.com
CyCraft secures government agencies, police and defense organizations, Fortune Global 500 firms, top banks and financial institutions, critical infrastructure, airlines, telecommunications, hi-tech firms, SMEs, and more by being Fast / Accurate / Simple /

Thorough.

CyCraft powers SOCs using innovative AI-driven technology to automate information security protection with built-in advanced managed detection and response (MDR), global cyber threat intelligence (CTI), smart threat intelligence gateway (TIG) and network detection and response (NDR), security operations center (SOC) operations software, auto-generated incident response (IR) reports, enterprise-wide Health Check (Compromise Assessment, CA), Secure From Home (SFH), and Risk Intelligence (RiskINT) services. Everything Starts From Security.

Meet your cyber defense needs in the 2020s by engaging with CyCraft at **engage@cycraft.com**

Related Resources

- Read CyCraft research to on why Midsize enterprises should embrace MDR providers.
- Effective SOCs aren’t bought; they’re built from the ground up. Avoid costly mishaps by .
- CyCraft targeting Taiwan’s high-tech ecosystem. Read our full analysis and malware reversal.
- detected, contained, and eradicated multiple sophisticated cyberattacks targeting several Taiwan government agencies.
-