How Falcon Complete Disrupts eCrime Operators (WIZARD SPIDER)

crowdstrike.com/blog/how-falcon-complete-disrupts-ecrime-operators-wizard-spider/

Falcon Complete Team

June 22, 2021

In this blog, we describe a string of recent incidents in which the CrowdStrike Falcon Complete™ team observed a financially motivated eCrime operator (likely WIZARD SPIDER) use compromised external remote services (Microsoft Remote Desktop Protocol, or RDP) along with *Cobalt Strike* in an unsuccessful attempt to deploy ransomware. This activity indicates a notable increase in the adversary's tactics to include RDP brute forcing along with their more traditional modus operandi for initial access via phishing or leveraging their partner networks of access brokers.

We will provide a brief overview of the observed tactics, techniques and procedures (TTPs) in these cases along with an outline of the Falcon Complete team's approach to quickly detect and contain the interactive attacker before the threat actor was able to complete actions on objective.

Campaign TTPs Overview

In recent weeks, the Falcon Complete team has conducted several response operations to incidents involving compromised RDP credentials as an initial infection vector. This was followed by execution of reconnaissance commands, installation of *Cobalt Strike* and additional tooling.

CrowdStrike Intelligence assesses that the threat actor responsible for this activity is likely WIZARD SPIDER due to the following overlapping TTPs with WIZARD SPIDER activity clusters:

- *Cobalt Strike* stager DLLs executed from the victim's Music directory
- Network indicators identified via hunting for related samples and infrastructure exhibiting attributes of WIZARD SPIDER infrastructure
- Using nltest and net Windows utilities to conduct reconnaissance activity

This assessment carries low confidence.

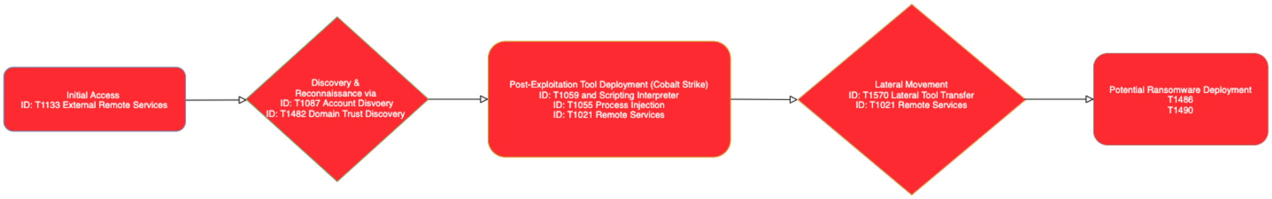
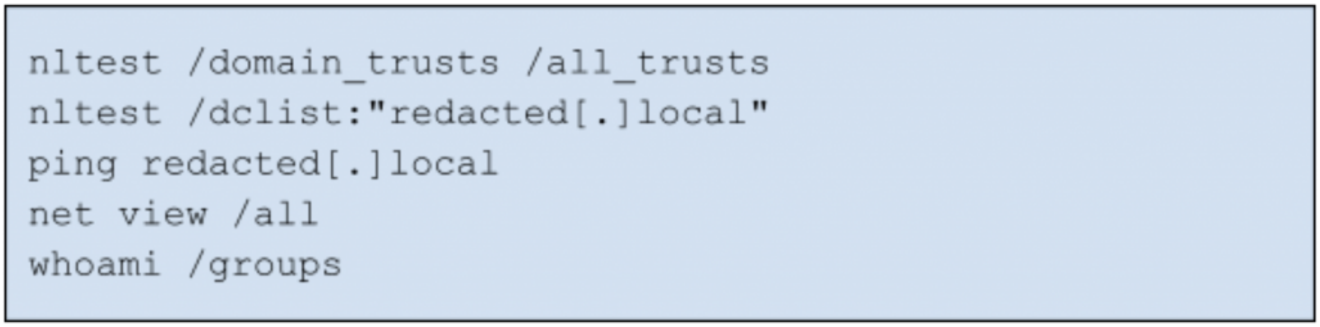

Initial Access
ID: T1133 External Remote Services
Discovery &
Reconnaissance via
ID: T1087 Account Disvoery
ID: T1482 Domain Trust Discovery
Post-Exploitation Tool Deployment (Cobalt Strike)
ID: T1059 and Scripting Interpreter
ID: T1055 Process Injection
ID: T1021 Remote Services
Lateral Movement
ID: T1570 Lateral Tool Transfer
ID: T1021 Remote Services
Potential Ransomware Deployment
T1486
T1490

Figure 1. Activity cluster patterns mapped to MITRE ATT&CK® (Click to enlarge)

WIZARD SPIDER is a criminal group behind the core development and distribution of a sophisticated arsenal of criminal tools, including the *Trickbot, BazarLoader, Conti* and *Ryuk* malware variants. This adversary has used big game hunting (BGH) tactics to great effect against a diverse set of targets across multiple sectors and geographies.

The typical activity patterns observed by the Falcon Complete team in recent intrusions include an initial attack vector via compromised external remote services — commonly, exposed RDP. This suggests a notable increase in this tactic. It is unclear whether the increased focus on external remote services is a shift away from phishing and using access brokers, or whether this is simply an addition to the adversary's overall modus operandi. Adversaries often obtain credentials in multiple ways, whether by brute forcing an externally exposed service, purchasing them on underground markets or conducting credential harvesting operations.

Once the actor has established a foothold within an environment, they will proceed with reconnaissance activities to enumerate accounts and systems that may represent high-value targets. Multiple reconnaissance commands were observed — in particular, nltest appears to be a hallmark of this activity. Shown in Figure 2, the adversary first enumerated the trusted domains in the environment, and then a list of domain controllers. Their goal was likely to move laterally to one of these systems.



```
nltest /domain_trusts /all_trusts
nltest /dclist:"redacted[.]local"
ping redacted[.]local
net view /all
whoami /groups
```

Figure 2. Example reconnaissance commands

The threat actor then installed additional tooling for post-exploitation activities. This typically included *Cobalt Strike* for command and control, where the stager DLLs were written to the user’s `Music` directory. BloodHound or Adfind were pulled down from an external resource for additional account enumeration in preparation for lateral movement. This secondary reconnaissance is handled by a BAT file written to the same `Music` directory.

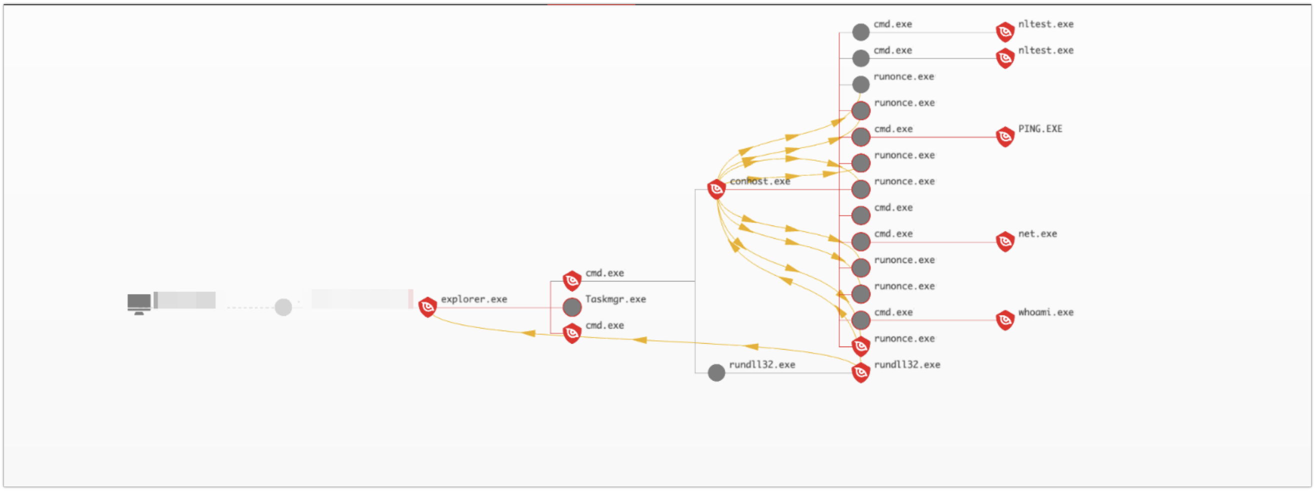


Figure 3. Process tree graph (Click to enlarge)

Figure 3 presents many of the common patterns related to the observed activity cluster as seen in the Falcon console. This process tree graph view indicates the initial process injection under the `explorer.exe` process via `rundll32.exe`, along with the initial reconnaissance commands such as `nltest` under the `conhost.exe` process.

Falcon Complete Detection and Response

Initial Detection and Triage

The Falcon Complete team has observed multiple related incidents over the past several weeks that share common TTPs, as noted above. Below, we present a case study of these contextual indicators observed during a specific incident.

The response process began when the Falcon Complete team received a high-severity machine learning (ML) detection for a suspicious process injection via `rundll32.exe`. Further investigation indicated that this process injection was related to the threat actor abusing Microsoft Office Visual Basic for Applications (VBA) macros in an uncommon way.

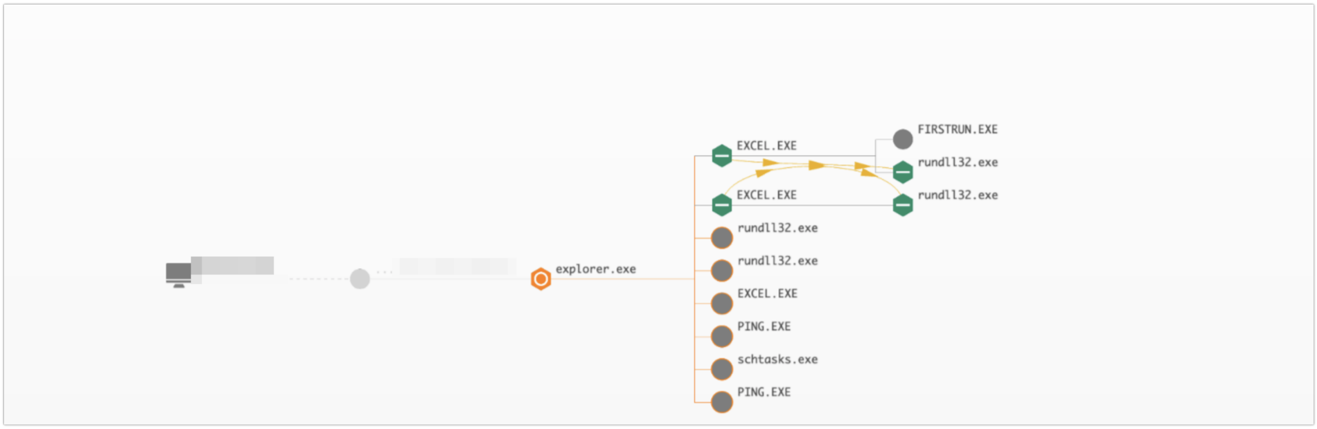
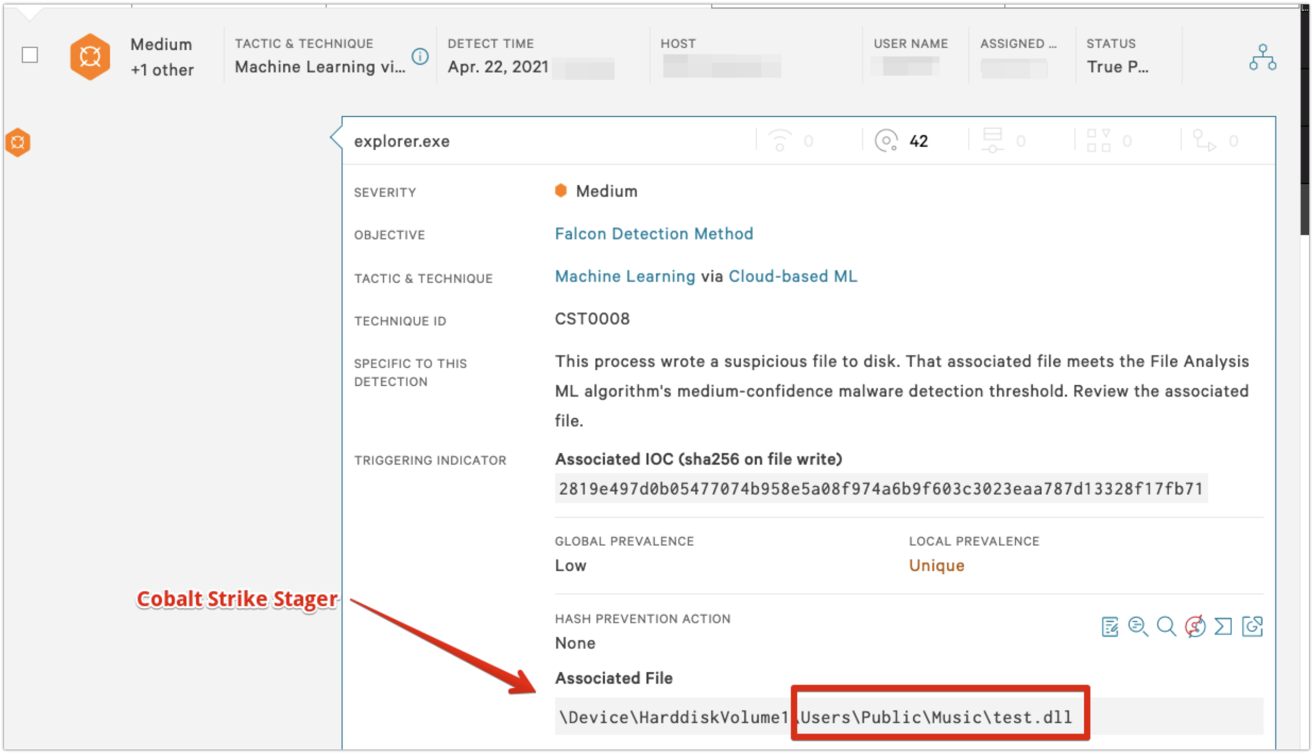


Figure 4. Process tree with Microsoft Excel copy/paste (Click to enlarge)

This shellcode was a typical stager that functioned as a downloader to fetch a *Cobalt Strike* payload from the attacker-controlled command and control (C2). These resources were written to the `C:\Users\Public\Music` directory.



☐ Medium +1 other | TACTIC & TECHNIQUE Machine Learning vi... | DETECT TIME Apr. 22, 2021 [redacted] | HOST [redacted] | USER NAME [redacted] | ASSIGNED ... [redacted] | STATUS True P...

explorer.exe 0 42 0 0 0

SEVERITY: Medium

OBJECTIVE: Falcon Detection Method

TACTIC & TECHNIQUE: Machine Learning via Cloud-based ML

TECHNIQUE ID: CST0008

SPECIFIC TO THIS DETECTION: This process wrote a suspicious file to disk. That associated file meets the File Analysis ML algorithm's medium-confidence malware detection threshold. Review the associated file.

TRIGGERING INDICATOR: **Associated IOC (sha256 on file write)**
`2819e497d0b05477074b958e5a08f974a6b9f603c3023eaa787d13328f17fb71`

GLOBAL PREVALENCE: Low

LOCAL PREVALENCE: Unique

HASH PREVENTION ACTION: None

Associated File
`\Device\HarddiskVolume1\Users\Public\Music\test.dll`

Figure 5. Detection showing *Cobalt Strike* stage location (Click to enlarge)

Adversaries utilizing Microsoft Office documents weaponized with VBA macros is nothing new, but the activity described above differs significantly from phishing campaigns leveraging macro documents to achieve initial access. Instead, the document was being used to execute code *after* initial access had been achieved on a system via a compromised account.

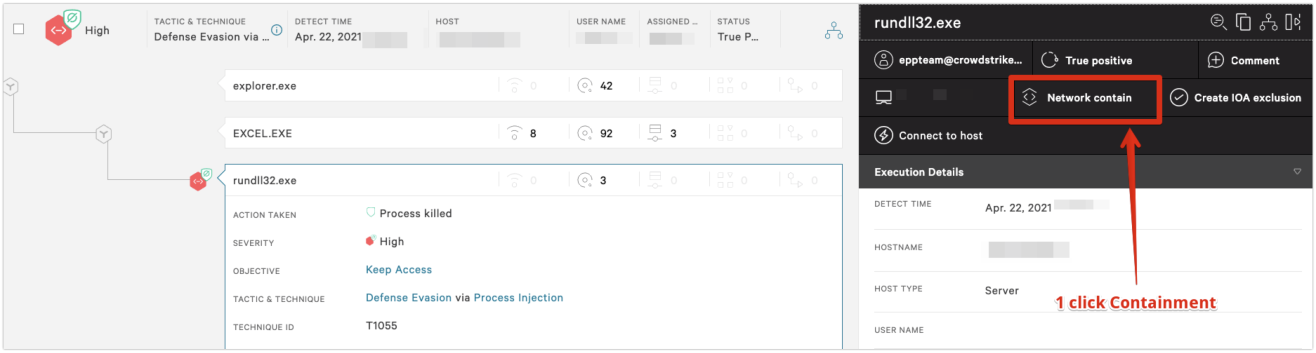
We have observed multiple instances of files written that were named either “New Microsoft Word Document.docx” or “New Microsoft Excel Worksheet.xlsx,” which are the default naming schemes for new document templates in Windows. Next, a macro executes a shellcode payload via the `rundll32.exe` process, which is a *Cobalt Strike* stager, but the macro’s shellcode is never written to disk.

This is likely an evasion technique attempting to bypass host-based security controls to execute shellcode. What appears to be happening is the threat actors are copying and pasting the malicious macro directly into a blank document template *over the RDP session*. The advantage of this approach is that the macros are not written to disk and are only executed in memory. This activity was then followed by similar reconnaissance commands observed in Figure 2 above.

Containment and Investigation

At this point, we were confident that an adversary was interactive and had compromised the victim host. We observed them attempting to perform reconnaissance in preparation for privilege escalation and lateral movement. The next steps were to contain and identify the full scope of the incident.

Our analysts have the capability to network-contain a host to prevent the lateral spread of the adversary within the environment. This immediately denies the adversary remote access by only allowing the host to communicate with the CrowdStrike Security Cloud.



	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNED ...	STATUS
High	Defense Evasion via ...	Apr. 22, 2021 [redacted]	[redacted]	[redacted]	[redacted]	True P...

explorer.exe	0	42	0	0	0
EXCEL.EXE	8	92	3	0	0
rundll32.exe	0	3	0	0	0

ACTION TAKEN: Process killed
SEVERITY: High
OBJECTIVE: Keep Access
TACTIC & TECHNIQUE: Defense Evasion via Process Injection
TECHNIQUE ID: T1055

rundll32.exe

eppteam@crowdstrike... | True positive | Comment
[redacted] | Network contain | Create IOA exclusion
Connect to host

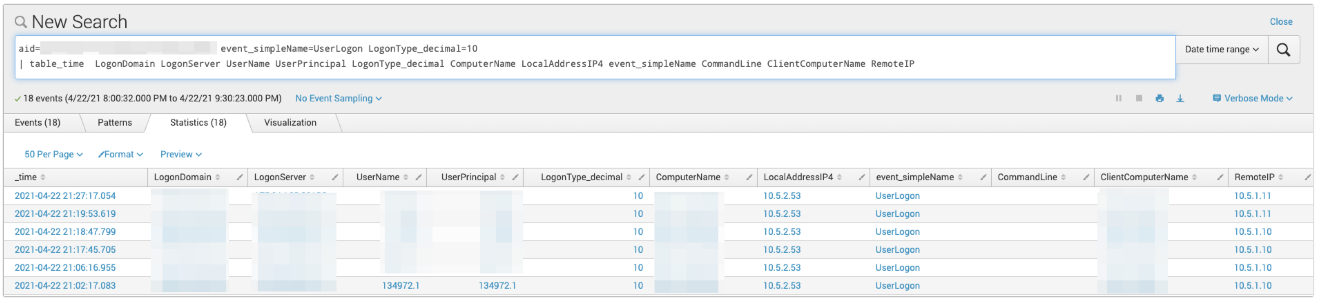
Execution Details

DETECT TIME: Apr. 22, 2021 [redacted]
HOSTNAME: [redacted]
HOST TYPE: Server
USER NAME

1 click Containment

Figure 6. Containment (Click to enlarge)

The next objective of the investigation was to properly scope the intrusion by identifying the affected systems/user accounts and host/network indicators of compromise. We can pivot into our endpoint activity monitoring (EAM) application, which provides endpoint telemetry so we can gain further context and determine the origin of the intrusion.



```
aid=[redacted] event_simpleName=UserLogon LogonType_decimal=10
| table_time  LogonDomain LogonServer UserName UserPrincipal LogonType_decimal ComputerName LocalAddressIP4 event_simpleName CommandLine ClientComputerName RemoteIP
```

✓ 18 events (4/22/21 8:00:32.000 PM to 4/22/21 9:30:23.000 PM)

_time	LogonDomain	LogonServer	UserName	UserPrincipal	LogonType_decimal	ComputerName	LocalAddressIP4	event_simpleName	CommandLine	ClientComputerName	RemoteIP
2021-04-22 21:27:17.054	[redacted]	[redacted]	[redacted]	[redacted]	10	[redacted]	10.5.2.53	UserLogon		[redacted]	10.5.1.11
2021-04-22 21:19:53.619	[redacted]	[redacted]	[redacted]	[redacted]	10	[redacted]	10.5.2.53	UserLogon		[redacted]	10.5.1.11
2021-04-22 21:18:47.799	[redacted]	[redacted]	[redacted]	[redacted]	10	[redacted]	10.5.2.53	UserLogon		[redacted]	10.5.1.10
2021-04-22 21:17:45.705	[redacted]	[redacted]	[redacted]	[redacted]	10	[redacted]	10.5.2.53	UserLogon		[redacted]	10.5.1.10
2021-04-22 21:06:16.955	[redacted]	[redacted]	[redacted]	[redacted]	10	[redacted]	10.5.2.53	UserLogon		[redacted]	10.5.1.10
2021-04-22 21:02:17.083	[redacted]	[redacted]	134972.1	134972.1	10	[redacted]	10.5.2.53	UserLogon		[redacted]	10.5.1.10

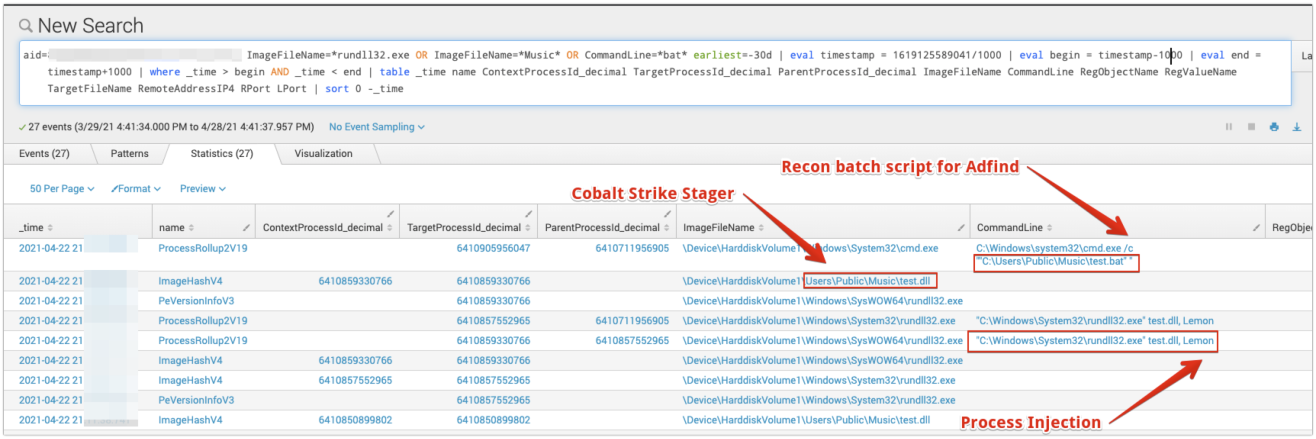
Figure 7. EAM query for type 10 logons (RDP) (Click to enlarge)

The goal here was determining the user account that the threat actor compromised and leveraged for remote access. In Figure 7, a simple query for `type 10` logons can determine this account. This query also gives us the `Remote` IP, which is the source host of the RDP logon. This information could also be gleaned from a Falcon Real Time Response (RTR) session on the host to query the security event logs via PowerShell, such as the following snippet:

```
Get-EventLog -LogName Security -InstanceId 4624 -Newest
10 | Select-Object -Property
entrytype,instanceID,TimeGenerated,Message
```

Figure 8. Alternative method for event logs

The EAM application can also be used to search for residual host artifacts that the adversary may have left behind on the system. From the initial detection triage, we can then pivot from data points such as the injected process, directory locations and specific file types of interest. A basic query is shown in Figure 9 to identify the artifacts of interest that remain on disk.



```
aid=[redacted] ImageFileName=*rundll32.exe OR ImageFileName=*Music* OR CommandLine=*bat* earliest=-30d | eval timestamp = 1619125589041/1000 | eval begin = timestamp-1000 | eval end =
    timestamp+1000 | where _time > begin AND _time < end | table _time name ContextProcessId_decimal TargetProcessId_decimal ParentProcessId_decimal ImageFileName CommandLine RegObjectName RegValueName
    TargetFileName RemoteAddressIP4 RPort LPort | sort 0 -_time
```

✓ 27 events (3/29/21 4:41:34.000 PM to 4/28/21 4:41:37.957 PM)

_time	name	ContextProcessId_decimal	TargetProcessId_decimal	ParentProcessId_decimal	ImageFileName	CommandLine	RegObje
2021-04-22 21[redacted]	ProcessRollup2V19		6410905956047	6410711956905	\Device\HarddiskVolume1\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\Users\Public\Music\test.bat" "	
2021-04-22 21[redacted]	ImageHashV4	6410859330766	6410859330766		\Device\HarddiskVolume1\Users\Public\Music\test.dll		
2021-04-22 21[redacted]	PeVersionInfoV3		6410859330766		\Device\HarddiskVolume1\Windows\SysWOW64\rundll32.exe		
2021-04-22 21[redacted]	ProcessRollup2V19		6410857552965	6410711956905	\Device\HarddiskVolume1\Windows\System32\rundll32.exe	"C:\Windows\System32\rundll32.exe" test.dll, Lemon	
2021-04-22 21[redacted]	ProcessRollup2V19		6410859330766	6410857552965	\Device\HarddiskVolume1\Windows\SysWOW64\rundll32.exe	"C:\Windows\System32\rundll32.exe" test.dll, Lemon	
2021-04-22 21[redacted]	ImageHashV4	6410859330766	6410859330766		\Device\HarddiskVolume1\Windows\SysWOW64\rundll32.exe		
2021-04-22 21[redacted]	ImageHashV4	6410857552965	6410857552965		\Device\HarddiskVolume1\Windows\System32\rundll32.exe		
2021-04-22 21[redacted]	PeVersionInfoV3		6410857552965		\Device\HarddiskVolume1\Windows\System32\rundll32.exe		
2021-04-22 21[redacted]	ImageHashV4	6410850899802	6410850899802		\Device\HarddiskVolume1\Users\Public\Music\test.dll		

Figure 9. EAM query for host artifacts (Click to enlarge)

Based on observations from previous intrusions, we knew that a batch file may be present in the same directory as the *Cobalt Strike* stager. As noted before, this batch file is responsible for conducting further reconnaissance with Adfind to explore the Active Directory environment. As shown in Figure 9, the EAM query also captured the command `rundll32.exe test.dll, Lemon`. This command is responsible and is used for process injection via `rundll32.exe`. Previously, the Falcon Complete team has observed similar patterns regarding one-word export functions such as *"Lemon"* in this case, and *"Lime"* in similar instances. These one-word export functions likely suggest a possible common naming convention for exports, related to *Cobalt Strike* DLLs across the intrusions observed. Investigators can use this indicator to pivot or enrich related data sets of potentially linked activity clusters.

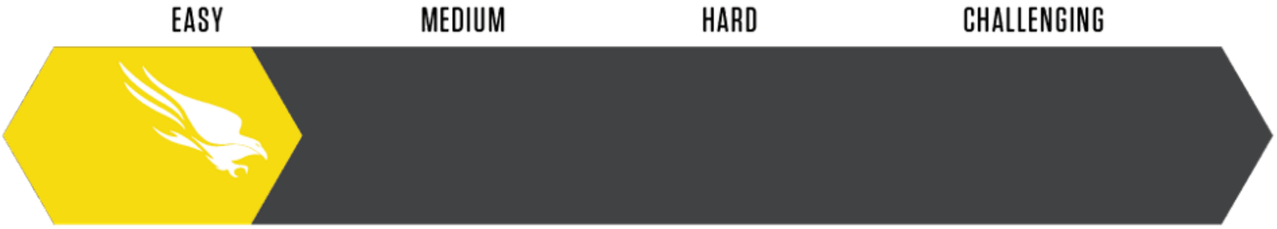
Next, the team performed dynamic malware analysis on the *Cobalt Strike* stager sample. We discovered that the binary's code was configured to reach out to the domain `serviapd[.]com` for C2. At this point in the investigation, we had determined both the system and user scopes, identified host artifacts and extracted network indicators of compromise (IOCs) from the malware. Armed with this information, the Falcon Complete team could now begin removing the actor's malware from the affected systems.

Remediation

The Falcon Complete team directly performs many of the critical remediation actions for our customers via Falcon RTR.

A typical remediation can be broken into three distinct steps:

1. Killing the malicious processes (e.g., injected rundll, explorer, conhost)
2. Locating and removing the persistence mechanism (e.g., compromised accounts, services)
3. Removing disk artifacts (e.g., binaries and directories)



In this case, we have rated this remediation as "Easy," based on the velocity and total effort required for proper recovery. Due to the rapid response time to contain and evict the adversary, there was not an extensive list of clean-up actions to be taken.

STEP 1. Finding and Killing the Malicious Process

Falcon did a lot of the work for us here and had already terminated the injected processes. The running process was reviewed to ensure no injected threads were still executing malicious code. We have provided more details for finding injected process in previous blogs:

- Automating Remote Remediation of TrickBot: Part 1
- Duck Hunting with Falcon Complete: Remediating a Fowl Banking Trojan, Part 3

STEP 2. Removing Persistence

The adversary did not have time (or didn't bother) to establish persistence beyond the compromised account credentials leveraged in the RDP session. We worked with the client to reset these accounts and harden remote services to avoid further exploitation. Our recommendations for best practices include:

- Using multifactor authentication (MFA) for remote access services
- Disabling RDP or any services that are not required
- Using non-standard ports if required
- Deploying technical controls such as Web Application Firewall (WAF) in front of remote services

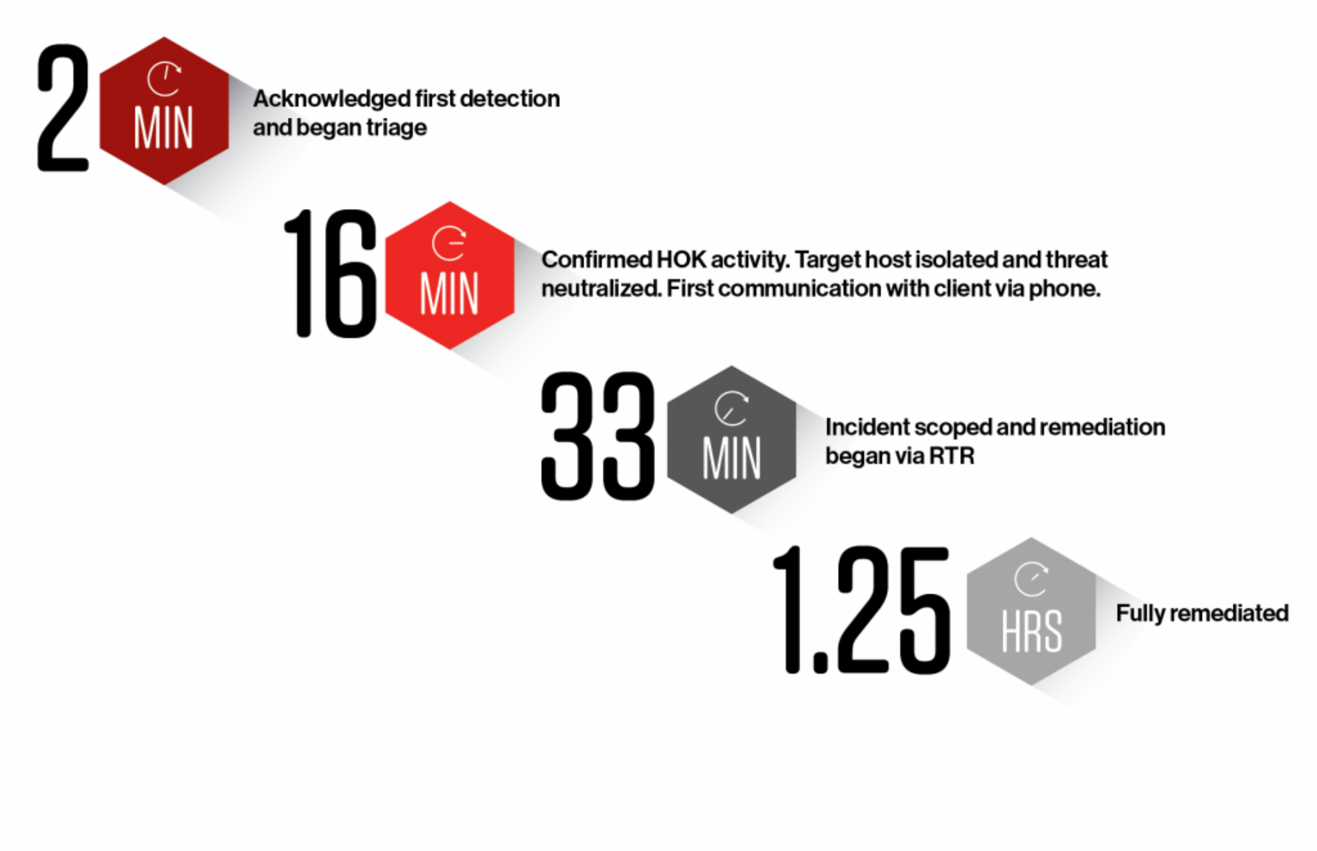
STEP 3. Removing Remaining Artifacts

Using Falcon RTR, we removed all adversary tooling and file system residue present in the `C:\Users\Public\Music` directory.

The steps outlined above are the general process for successfully remediating a host for the artifacts of this intrusion set.

The Efficiency of Falcon Complete

The Falcon Complete team identified an interactive adversary that had compromised an external remote service and gained illicit access to a managed host in our client's environment. This threat actor attempted to download and execute additional tooling in a likely attempt to stage ransomware. The team quickly contained, scoped and remediated this threat with the Falcon RTR capability without requiring any reboots, reimages or other disruption to the client's business operations. The following figure highlights the significant milestones during our detection and response efforts.


2 MIN
Acknowledged first detection and began triage
16 MIN
Confirmed HOK activity. Target host isolated and threat neutralized. First communication with client via phone.
33 MIN
Incident scoped and remediation began via RTR
1.25 HRS
Fully remediated

Response When Minutes Matter: Falcon Complete Disrupts eCrime Operators

This activity was attributed to the financially motivated adversary tracked as WIZARD SPIDER.

The Falcon Complete team has observed multiple similar TTPs in several recent intrusions that indicate a general tactical increase or preference for compromising external remote services (such as RDP) as an initial infection vector. It is unclear but possible that this activity is simply in addition to this actor's "normal" email phishing operations. We also noted an interesting usage of a technique leveraging Microsoft Office macros following initial access. It is likely that eCrime actors will continue to use this technique going forward. The Falcon Complete team will continue to track this threat and monitor our clients' environments for any notable developments.

Additional Resources

- *Read more blogs from the Falcon Complete team: Falcon Complete Disrupts Malvertising Campaign Targeting AnyDesk, Response When Minutes Matter: Rising Up Against Ransomware and Falcon Complete Stops Microsoft Exchange Server Zero-Day Exploits.*
- *Learn more by visiting the Falcon Complete product webpage.*
- *Read a white paper: CrowdStrike Falcon Complete: Instant Cybersecurity Maturity for Organizations of All Sizes.*