Shifting in the Wind: WINDSHIFT Attacks Target Middle Eastern Governments

unit42.paloaltonetworks.com/shifting-in-the-wind-windshift-attacks-target-middle-eastern-governments/

Adrian McCabe February 21, 2019

By Adrian McCabe

February 21, 2019 at 6:00 AM

Category: Unit 42, Unit 42

Tags: Mac, Middle East, OSX, WINDSHIFT

This post is also available in: 日本語 (Japanese)

Executive Summary

In August of 2018, DarkMatter released a report entitled "In the Trails of WINDSHIFT APT", which unveiled a threat actor with TTPs very similar to those of Bahamut. Subsequently, two additional articles (here and here) were released by Objective-See which provide an analysis of some validated WINDSHIFT samples targeting OSX systems. Pivoting on specific file attributes and infrastructure indicators, Unit 42 was able to identify and correlate additional attacker activity and can now provide specific details on a targeted WINDSHIFT attack as it unfolded at a Middle Eastern government agency.

Summary of Aggregated WINDSHIFT Attacker Activity

The following timeline summarizes validated WINDSHIFT activity through June of 2018.

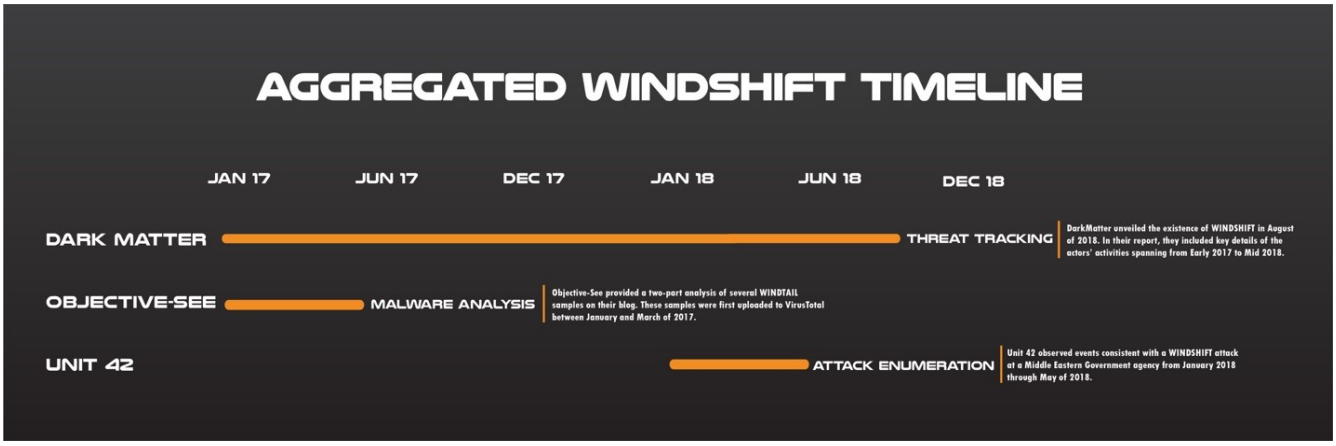

Figure 1: Known WINDSHIFT activity across main disclosure sources.

As shown within the timeline above, the WINDSHIFT activity observed by Unit 42 falls between January and May of 2018.

Middle Eastern Government Agency Attack Timeline

The following is a summary of observed WINDSHIFT activity which targeted a Middle Eastern government agency:

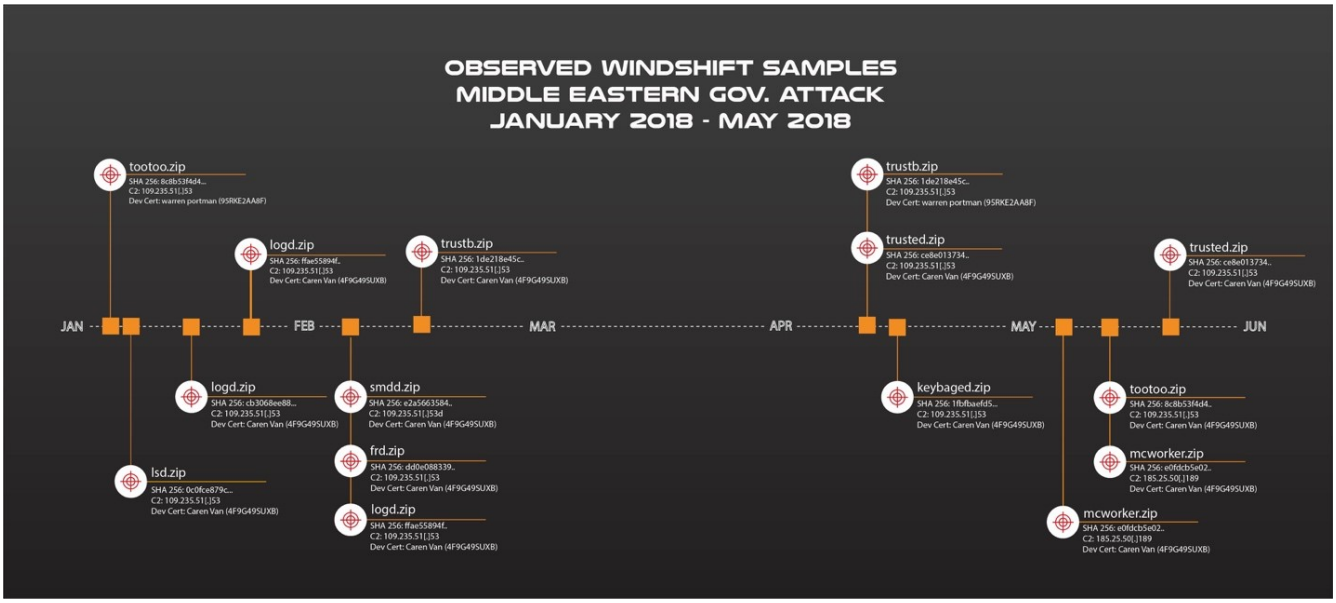

Figure 2: Unit 42 Observed WINDSHIFT samples.

The first attack occurred in early January of 2018 with an inbound WINDTAIL sample (the backdoor family used by WINDSHIFT) originating from the remote IP address 109.235.51[.]110 to a single internal IP address within the government agency. As per the timeline in Figure 2, at the time this event occurred, the IP address 109.235.51[.]110 was associated with the domain flux2key[.]com, a known WINDSHIFT domain. Upon further analysis, Unit 42 determined the sample's corresponding C2 server IP address was 109.235.51[.]153. At the time this event occurred, that IP was associated with the domain string2me[.]com, which is a known WINDSHIFT domain. While Unit 42 does not have any insight into the attempted infection methodology in this case, the actor's TTPs would suggest that spearphishing was almost certainly involved.

After the initial infection attempt, several additional WINDTAIL samples from the same external IP address, 109.235.51[.]110, were directed at the same internal IP address from January through May of 2018 (see Figure 2 for additional details). All related WINDTAIL samples were Mac OSX app bundles in zip archives, which is consistent with WINDSHIFT TTPS.

One sample in particular, named "mcworker.zip" (SHA256: e0fdcb5e0215f9fae485fbfcd615c79b85806827e461bca2e1c00c82e83281dc) deserves particular attention. Upon further analysis, Unit 42 determined its C2 server IP address was 185.25.50[.]189. According to OSINT, at the time of the activity, the IP address 185.25.50[.]189 had one domain resolution: domforworld[.]com.

Conclusion

By analyzing this attack in detail, Unit 42 was able to gain valuable insight into the real-world TTPs of a known threat actor group. Of particular importance are the following findings:

- Unit 42 assesses with high confidence that both the IP address 185.25.50[.]189 and the domain domforworld[.]com is associated with WINDSHIFT activity. Additionally, the IP addresses 109.235.51[.]110 and 109.235.51[.]153, corresponding to the previously validated WINDSHIFT domains flux2key[.]com and string2me[.]com, respectively, were also observed in use during this campaign.

- The attacker-owned IP address 109.235.50[.]191 was subsequently identified in a Norman Security report from as being associated with Hangover threat actor activity, and both IP addresses 109.235.51[.]110 and 109.235.50[.]191 shared the name “XENEUROPE” within their organizational registrant WHOIS information. This organizational name is tied to a number of IP addresses of Hangover-associated infrastructure as per the Norman report. Collectively, this evidence serves to strengthen the implication from other security researchers that Operation Hangover and WINDSHIFT activity are possibly related.
- Based on Unit 42’s observations of multiple inbound WINDTAIL samples directed at the same internal IP address, Unit 42 assesses with moderate confidence that the attackers were not able to establish persistence within the targeted environment. While Unit 42 cannot definitively determine the attempted delivery vector of these samples, WINDTAIL TTPs would indicate that it was likely standard spearphishing chicanery.
- One of two of the Mac OSX developer certificates tied to the WINDTAIL samples shown in DarkMatter’s original presentation, Caren Van (4F9G49SUXB), was also tied to the WINDTAIL samples within this blog. Additionally, a newly identified certificate, warren portman (95RKE2AA8F), was found to be directly affiliated with WINDSHIFT malware.

Palo Alto Networks customers are protected from this threat in the following ways:

- AutoFocus customers can track these samples with the Windshift tag.
- WildFire detects all files mentioned in this report with malicious verdicts.

IOCs

Infrastructure:

Domain	IP Address
flux2key[.]com	109.235.51[.]110
string2me[.]com	109.235.51[.]153
domforworld[.]com	185.25.50[.]189

File Hashes:

File Name(s)	Apple Developer Certificate	SHA-256
trusted.zip	Caren Van (4F9G49SUXB)	ce8e01373499b539f4746c0e68c850357476abe36b12834f507f9ba19af3d4f9
mcworker.zip	Caren Van (4F9G49SUXB)	e0fdcb5e0215f9fae485fbfcd615c79b85806827e461bca2e1c00c82e83281dc
keybaged.zip	Caren Van (4F9G49SUXB)	1fbfbaefd50627796e7f16b8cc2b81ffbc5effcb33b64cc8e349e44b5d5d3ee8
trustb.zip	Caren Van (4F9G49SUXB)	1de218e45cdf069c10d1a8735d82688b8964261a5efe3b6560e0fdcfa3c44c1d
frd.zip	Caren Van (4F9G49SUXB)	dd0e0883392ffe8c72c4b13f58e5861fc2f4bc518a6abea4f81ae3a44b2eda1c

smdd.zip	Caren Van (4F9G49SUXB)	e2a5663584727efa396c319f7f99a12205bb05c9c678ffae130e9f86667505a6
logd.zip	Caren Van (4F9G49SUXB)	ffae55894f0f31d99105b5b7bbbca79e9c1019b37b7a5a20368f50c173352fd1
logd.zip	Caren Van (4F9G49SUXB)	cb3068ee887fc2f66d3df886421d5e5fa5e31ec4ee0079a7dcf9628bd2730de0
lsd.zip	Caren Van (4F9G49SUXB)	0c0fce879c8ca00a6f9feeaccf6cba64374e508cacd664682e794a4a4cc64ffb
tootoo.zip	warren portman (95RKE2AA8F)	8c8b53f4d4836bd7d4574fe80039caf9f2bd4d75740f2e8e22619064c830c6d9

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.