



TDROP2 ATTACKS SUGGEST DARK SEOUL ATTACKERS RETURN

153
Like

Tweet
0
G+

POSTED BY: [Bryan Lee](#) and [Josh Grunzweig](#) on November 18, 2015 4:25 PM

FILED IN: [Malware](#), [Threat Prevention](#), [Unit 42](#)
TAGGED: [AutoFocus](#), [Dark Seoul](#), [Operation Troy](#), [TDrop](#), [TDrop2](#), [WildFire](#)

While researching new, unknown threats collected by WildFire, we discovered the apparent re-emergence of a cyber espionage campaign thought to be dormant after its public disclosure in June 2013. The tools and tactics discovered, while not identical to the previous Dark Seoul campaign, showed extreme similarities in their functions, structure, and tools. In this post, we will provide an overview of the original Dark Seoul campaign in 2013, the similarities and differences in tactics, the malware used, as well as attempt to answer the question of 'why now'?

OVERVIEW

In March 2013, the country of South Korea experienced a major cyberattack, affecting tens of thousands of computer systems in the financial and broadcasting industries. This attack was dubbed 'Dark Seoul'; it involved wreaking havoc on affected systems by wiping their hard drives, in addition to seeking military intelligence.

The attack was initially thought to be attributed to North Korea, by way of a Chinese IP found during the attack, but no other strong evidence of North Korea's involvement has been produced since then. In June 2013, McAfee published a report detailing the chronology and variance of the Dark Seoul campaign, but renamed it 'Operation Troy'. The report analyzed the entirety of the purported attack campaign, beginning in 2009 using a family of tools dubbed 'Troy'. McAfee further attributed two groups to the campaign: the NewRomanic Cyber Army Team and The Whois Hacking Team; both groups believed to be state sponsored. Since the publication of that report, no other activity involving either group or the tools have been detected or shared publically.

That is, until now.

DARK SEOUL RETURNS

Using the Palo Alto Networks [AutoFocus threat intelligence platform](#), we identified several samples of malicious code with behavior similar to the aforementioned Operation Troy campaign dating back to June 2015, over two years after the original attacks in South Korea. Session data revealed a live attack targeting the transportation and logistics sector in Europe. The initial attack was likely a spear-phishing email, which leveraged a trojanized version of a legitimate software installation executable hosted by a company in the industrial control systems sector. The modified executable still installs the legitimate video player software it claims to contain, but also infects the system. Based on deep analysis of the Trojan's behavior, binary code, and previous reports of similar attacks, we have concluded that these samples were the same as the original tools used in the Dark Seoul/Operation Troy attacks. It is likely the same adversary group is involved, although there is currently insufficient data to confirm this conclusion.

MALWARE OVERVIEW

The malicious code was delivered via the following two executable names, packaged together in a zip archive file:

- [redacted]Player_full.exe
- [redacted]Player_light.exe

Both executables present themselves as legitimate installation programs offered by the industrial control systems organization, providing video player software for security camera solutions. When either sample was executed, the malware dropped and subsequently executed the actual video player it disguised itself as.

The new malware variant, which we call TDrop2, proceeds to select a legitimate Microsoft Windows executable in the system32 folder executes it, and then uses the legitimate executable's process as a container for the malicious code, a technique known as process hollowing. Once successfully executed, the corresponding process then attempts to retrieve the second-stage payload.

- Home
- Government
- Partners
- Unit 42 Threat Intelligence
- Technical Documentation
- Advanced Endpoint Protection



Get Updates
Sign up to receive the latest news, cyber threat intelligence and research from Unit 42.

SUBSCRIBE TO THE RESEARCH CENTER BLOG

CATEGORIES & ARCHIVES

[MORE →](#)

RECENT POSTS

[Upatre: Old Dog, New \[Anti-Analysis\] Tricks](#)
posted by [Brandon Levene](#) on November 20, 2015

[Channel Scoop – November 20, 2015](#)
posted by [Lang Tibbils](#) on November 20, 2015

[Get Your Copy of Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers](#)
posted by [Anna Lough](#) on November 19, 2015

[Fuel User Group: Your Membership Questions Answered](#)
posted by [Megan Scofield](#) on November 19, 2015

[TDrop2 Attacks Suggest Dark Seoul Attackers Return](#)
posted by [Bryan Lee](#) on November 18, 2015

[MORE →](#)

different in that this observed attack is not aimed at military, government, or financial institutions in the South Korea region. In addition, there has been no evidence of destructive functionality in the samples analyzed by Unit 42, although the malware is capable of downloading additional components so those simply may not yet have been observed.

The similarities in tactics however, do seem to outweigh the differences, and it is highly likely this is the same group or groups responsible for the original Dark Seoul/Operation Troy attacks, but with a new target and a new campaign.

CONCLUSION

It is not uncommon for threat actors to become dormant for some period of time, especially after public unveiling as the groups behind Dark Seoul/Operation Troy experienced. What we do know is that changing infrastructure and toolsets can be challenging, and it is not nearly as common that a very specialized tool developed for specific teams would be shared amongst threat actors.

There is insufficient data at this time to clearly state why Dark Seoul/Operation Troy would resurface at this time, but Unit 42 will continue to monitor the activity as the situation develops.

We have created the AutoFocus tag **TDrop2** to identify samples of this new variant and have added known C2 domains and hash values to the Threat Prevention product set. At this time, WildFire is able to correctly identify the samples associated with this campaign as malicious.

IOC LIST

SHA256 HASHES

```
52939b9ec4bc451172fa1c5810185194af7f5f6fa09c3c20b242229f56162b0f
1dee9b9d2e390f217cf19e63cdc3e53cc5d590eb2b9b21599e2da23a7a636184
52d465e368d2cb7dbf7d478ebadb367b3daa073e15d86f0cbd1a6265abfbd2fb
a02e1cb1efbe8f3551cc3a4b452c2b7f93565860cde44d26496aabd0d3296444
43eb1b6bf1707e55a39e87985eda455fb322afae3d2a57339c5e29054fb52042
```

DOMAINS

```
www.junfac[.]com
www.htomega[.]com
mcm-yachtmanagement[.]com
www.combra[.]eu
```

URLS

```
www.junfac[.]com/tires/skin/tires.php
www.htomega[.]com/rgboard/image/rgboard.gif
mcm-yachtmanagement[.]com/installx/install_ok.php
www.combra[.]eu/includes/images/logo.jpg
```



14 PINGBACKS & TRACKBACKS

November 18, 2015 10:10 PM

[Hacking group that hit South Korea may be at it again with new target | SplitReads](#)

November 18, 2015 10:14 PM

[Hacking group that hit South Korea may be at it again with new target - GeekTechTalk](#)

November 18, 2015 10:45 PM

[Hacking group that hit South Korea may be at it again with new target | Technewsnow.Today](#)

November 18, 2015 11:28 PM

[Hacking group that hit South Korea may be at it again with new target | Virus / malware / hacking / security news](#)

November 19, 2015 2:08 AM

[Hacking group that hit South Korea may be at it again with new target | fairtechsupport.com](#)

November 19, 2015 4:33 AM

[Hacking group that hit S. Korea may be at it again with new target | Ian Young's Blog](#)

November 19, 2015 5:09 AM

[Hacking group that hit S. Korea may be at it again with new target | Technewsnow.Today](#)

November 19, 2015 5:10 AM

[Hacking group that hit South Korea may be at it again with new target | Templar Shield](#)

November 19, 2015 5:30 AM

[Hacking group that hit S. Korea may be at it again with new target - News Press](#)

November 19, 2015 6:07 AM

[Hacking group that hit S. Korea may be at it again with new target | PHP](#)

November 19, 2015 7:06 AM

[Hacking group that hit South Korea may be at it again with new target | Computer network knowledge](#)

November 19, 2015 7:09 AM

[Attacks on European Firms Suggest Return of "Dark Seoul" Group | Cyber Security News](#)

November 19, 2015 7:35 AM

[Hacking group that hit South Korea may be at it again with new target | Network World](#)

November 19, 2015 1:36 PM

[Hacking group that hit South Korea may be at it again with new target | IP Pings](#)

POST YOUR COMMENT

Name *

Email *

Website