

Novel Excel Spreadsheet Attack Launches Password Stealing Malware Loki Bot

lastline.com/blog/password-stealing-malware-loki-bot/

December 19, 2017



Posted by [Lastline](#) ON DEC 19, 2017

Lastline has uncovered a new attack vector launched through Microsoft Excel spreadsheets, and just recently expanded into other Office applications. The challenge is not only the novel technique used but also the difficulty in detecting it in its early stages. Too often companies, due to lack of malware behavior analysis, dismiss alerts as false positives, losing precious time during which the malware is busy stealing credentials. In this post, we'll describe how the attack works, and what typically happens during the initial days of the attack.

The Attack and the Payload: Dissected

Recently Lastline Labs published a [blog post](#) titled “When Scriptlets Attack,” about a trending new infection method in Microsoft Excel spreadsheets that we first saw on the 29th of November. As per the earlier blog post, we scanned the file on Virustotal and only three tools

detected it as malicious.

With such a low detection rate of this method of attack, many organisations would be at the mercy of the scriptlets payload. Indeed with only three detections, many would consider the original Excel infection vector to be a false positive and do no further investigation or remediation of this attack. The payload that is delivered by the Excel scriptlet is Loki, a notorious credential stealer malware tuned to focus on exfiltrating usernames and passwords (see Figure A).

Get TheLatest Loki Bot - Loki Botnet, Password Stealer, best tools for Alibaba And Wire Wire

August 23, 2017

Loki Bot or botnet with Resident Loader and Password Stealer, best tools for Alibaba And Wire Wire.


It is clear that this new **Loki Bot** is capable of stealing credentials from more than 100 different software tools (if installed.) In this section. The Loki Bot has been observed for years. As you may know, it is designed to steal credentials from installed software on a victim's machine, such as email clients, browsers, FTP clients, file management clients, and so on.



Figure A: Dark web ad promoting Loki Bot malware for stealing credentials

This is a double whammy for most security response teams. Firstly, the low detection rate of the infection vector would lean people towards a False Positive verdict. And secondly, even if they discovered the main payload, Loki, mitigating the behaviour of the threat is often incorrectly implemented. This leaves the victimized organisation open to a secondary malware-less attack when the exfiltrated credentials are used by subsequent threat actors to gain unauthorised access and then try to move around inside the network.

Fast forward nearly two weeks. As of 10 December, 12 days later after the first submission, the malicious Excel scriptlet spreadsheet has attracted 12 positive verdicts on Virustotal out of nearly 60 AV tools (see Figure B).



12 / 59

12 engines detected this file


SHA-256: dcd41be6e979b8ea95204ab4f9892e96a28db38378a41088b824967db8754662

File name: PAYMENT DETAILS.xlsx

File size: 7.43 KB

Last analysis: 2017-12-11 14:39:16 UTC

Community score: -1



Detection

Details

Relations

Community 2

Engine	Signature	Engine	Signature
AegisLab	⚠ Exploit.Msoffice.Generic	Ikarus	⚠ Win32.Outbreak
Kaspersky	⚠ HEUR:Exploit.MSOffice.Generic	McAfee	⚠ W97M/Downloader
McAfee-GW-Edition	⚠ W97M/Downloader	Microsoft	⚠ TrojanDownloader.O97M/Exforlet.A
Qihoo-360	⚠ susp.exp.20170199	Symantec	⚠ Trojan.Mdropper
TrendMicro	⚠ TROJ_POWLOAD.AUSJSU	TrendMicro-HouseCall	⚠ TROJ_POWLOAD.AUSJSU
ViRobot	⚠ XLS.Z.Agent.7608	ZoneAlarm	⚠ HEUR:Exploit.MSOffice.Generic
Ad-Aware	✔ Clean	AhnLab-V3	✔ Clean
Alibaba	✔ Clean	ALYac	✔ Clean
Antiy-AVL	✔ Clean	Arcabit	✔ Clean
Avast	✔ Clean	Avast Mobile Security	✔ Clean
AVG	✔ Clean	Avira	✔ Clean

Figure B: Twelve days after initial detection, 12 AV tools detected this threat

The situation, now that AV tools have caught up, is that security teams suddenly receive an alert from an AntiVirus scan in the internal environment, and they start the validation process. In gathering intelligence on the file, they would see that it now has 12 positive detections, and this level takes it over the line from a false positive to a possible malware infection. Starting 12 days after the initial infection, they would try to build evidence of the behaviour of the potential victim's system and match it against any IoCs stemming from the original Excel document. The team would have to track back through various logs until they found a connection to a Gabon Top Level Domain [.ga] website, offered from a free web hosting service that downloaded an executable file – `_output23476823784.exe` – to the victim (see Figure C). Provided with this information, they would instigate a further scan for the second stage payload, or hunt for known IoCs of the payload.

Index of /kitru/



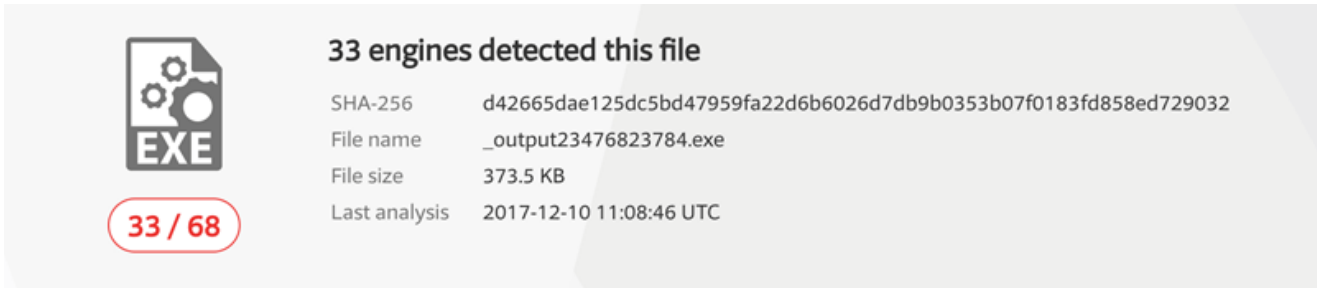
Name	Last modified	Size	Description
 Parent Directory	06-Dec-2017 06:10	-	
 _output23476823784.exe	06-Dec-2017 06:07	376k	
 scntanivia.xml	06-Dec-2017 05:26	12k	
 throni	06-Dec-2017 06:10	16k	

Figure C

Confirmation of a file hash on the local system would then be reinforced with further intelligence validation. The file `_output23476823784.exe` was unknown to VirusTotal before the 10 December. However, at Day 12 we have roughly 50% of detection engines returning positive convictions of .exe malware file that was delivered by the Excel scriptlet.



The image shows a VirusTotal analysis card for the file `_output23476823784.exe`. On the left, there is an icon of a document with gears and the text 'EXE', and a red badge indicating '33 / 68' detections. To the right, the title '33 engines detected this file' is followed by a table of file details.

SHA-256	d42665dae125dc5bd47959fa22d6b6026d7db9b0353b07f0183fd858ed729032
File name	_output23476823784.exe
File size	373.5 KB
Last analysis	2017-12-10 11:08:46 UTC

Now that we have a confirmed infection of the host, remediation action can begin. The vast majority of Anti-Virus labels (see Figure E) for the `_output23476823784.exe` payload indicate that it is a Trojan.Generic variety of payload. There are various discussed methods of remediating a generic Trojan infection including using cleanup tools from AntiVirus vendors, or as is often the case, a simple re-image of the system.
















 Trojan.GenericKDZ.41418
 Trojan.Generic.DA1CA
 FileRepMetagen [Malware]
 Win32.Trojan.WisdomEyes.16070401....
 malicious_confidence_90% (D)
 Unsafe
 Trojan.GenericKDZ.41418 (B)
 Trojan.GenericKDZ.41418
 Trojan.GenericKDZ.41418
 Trojan.GenericKDZ.41418
 HEUR:Trojan.MSIL.Generic
 Artemis!0AD49ADF19AB
 Trj/GdSda.A
 static engine - malicious
 heuristic

Figure E: AV tools identified the malware as a generic Trojan

To summarize, as of the end of Day 12, we found an infected client with a malicious Excel spreadsheet that communicated with a domain and installed a generic Trojan, which was subsequently detected and the client system was reimaged. Further studying of logs found

that the generic Trojan made some callbacks to a C&C server, but no lateral movement was seen, and a decision was made to close the incident.

Detection Balance, not Bias

Two pieces of conventional wisdom have driven the industry into this response process:

1. Prevention is better than a cure.

Nobody wants to be known as a “traditional security vendor” that cannot keep pace with the massive quantities of unique malware being produced. Instead, the Security industry has devised new detection methods to prevent malware from entering systems based in part on AI and ML, to statically determine good or bad elements of a file ... This is fine if the goal is to try to prevent 100% of attacks from ever entering the organisation. It’s a natural preference to simply stop malicious attacks entering the internal network, the problem is, when you miss one, it becomes very hard to triage and mitigate threats if all you have a heuristic alert produced by static analysis at the gateway.

2. Nobody wants malicious software to run in a production environment.

In attempting to address the quantity of detections issue, we, the security industry, have sacrificed quality of detections. We need to enrich our static protections with dynamic behavioural analysis to provide better protection for the attacks that breach defences. You need a malware analysis platform to do this.

Figure F shows the actual capabilities or behaviours of the Trojan.generic file `_output23476823784.exe` that was downloaded from the Excel spreadsheet. We can see that this Trojan is heavily weighted to stealing passwords. If our detection and remediation processes rely on static detections to alert and have no behavioural intelligence, then we are incorrectly closing incidents that still pose a significant risk.

Analysis Overview

Severity	Type	Description
99	Network	Command&Control traffic observed
80	Steal	Reading FTP client credentials
50	Memory	Replacing the image of a process with the same original executable (potential unpacking)
45	Steal	Password brute-forcing capabilities (database servers)
40	Steal	Reading browser stored credentials (Safari)
40	Steal	Reading browser stored credentials (Opera)
40	Steal	Reading browser stored credentials (Internet Explorer)
40	Steal	Reading browser stored credentials (Firefox)
25	Steal	Targeting Windows Saved Credential
25	Steal	Targeting Outlook Mail Password
25	Steal	Targeting Internet Explorer Browser Password
25	Steal	Targeting Firefox Browser Password
25	Memory	Suspicious APIs Strings
20	Network	Requesting unreachable HTTP link
15	Settings	Granting rights to debug or read memory of another process (SeDebugPrivilege)
15	Search	Searching for Firefox Security module database
15	Search	Searching for Firefox Security Certificates
15	Search	Searching for Firefox Key Database
15	Search	Retrieving the user account name
15	Search	Enumerating keys related to FTP clients
10	Steal	Targeting Mozilla stored passwords

Figure F: Lastline’s behavioral analysis of the downloaded file


Behavioral Intelligence is the ability to point security operations at clear, concise remediation instructions. The Behavioral Intelligence Quotient (BIQ) is improved by extracting the purpose and intent of any potentially malicious encounter. The higher the BIQ in an organisation, the faster threat containment occurs using optimal resources with minimum impact.


Getting to Know the Payload: Loki Bot

The payload in question is further identified by behavioral intelligence as Loki bot. Below (Figure G) is a Dark Market advert for Loki.

01-16-2017, 05:01 PM

Psychiatrist
Senior Member



Join Date: Jan 2017
Posts: 1,271
Thanks ↗: 0
Thanks ↙: 0
Thanked in: 0 Posts
Country: 

Loki Bot - Resident Loader and Password Stealer (C++ bot)

I am promoting this for my trusted friend. i tested his service and it was nice. so i promote for him. read below.

I Setup Loki Bot - Resident Loader and Password Stealer

Loki Bot is resident loader and password stealer. It comes with wallet checker (coin inspector, read below). It can steal passwords from browsers, ftp/ssh, e-mail and poker clients. Written in C++. Works on Windows 2003, 2008, 2012, XP, Vista, 7, 8, 8.1, 10 and Linux. UAC bypass.

I provide a demo test for you to test it and see how it works before purchase more info and screenshots here: <https://lokipony.blogspot.com/>

Figure G: Dark Market Ad

Promotional videos of Loki, (see Figure H) demonstrate its prowess at capturing credentials from various applications, especially FireFox (47% of the stolen credentials) and Chrome (41%), while Windows and email credentials make up only 1-3%.







Top Client List	
 Mozilla Firefox	388 (47.7%)
 Google Chrome	339 (41.7%)
 Chromium	17 (2.1%)
 Opera (NEW)	15 (1.8%)
 FileZilla	13 (1.6%)
Windows Credentials	11 (1.4%)
AI RoboForm	10 (1.2%)
 Mozilla Thunderbird	7 (0.9%)
Outlook	5 (0.6%)
Sticky Notes	5 (0.6%)

Figure H: A screenshot from a Loki promotional video

Once credentials have been stolen from a victim, Loki displays which sites are now vulnerable to identity theft (see Figure I). These include social media sites, payment portals, bitcoin wallets, and even a Moroccan government login.

Data	Application	Report	Date
...e3@www.facebook.com	Internet Explorer	Open	2016-12-25 00:26:16
...r.com/index.php	Google Chrome	Open	2016-12-25 00:26:16
...2e3r4t5y6@www.bitzfree.com	Mozilla Firefox	Open	2016-12-25 00:26:16
...com	Mozilla Firefox	Open	2016-12-25 00:26:16
...ourtranslation.com	Mozilla Firefox	Open	2016-12-25 00:26:16
...Jodhj123@myaccount.payoneer.com	Mozilla Firefox	Open	2016-12-25 00:26:16
...	Mozilla Firefox	Open	2016-12-25 00:26:16
...Jodhj123456@ojo.cash	Mozilla Firefox	Open	2016-12-25 00:26:16
...	Mozilla Firefox	Open	2016-12-25 00:26:16
...kFahoaQfB@freembitco.in	Mozilla Firefox	Open	2016-12-25 00:26:16
...22eb8cd5e7.a1z2e3r4t5y6@blockchain.info	Mozilla Firefox	Open	2016-12-25 00:26:16
...y.com	Mozilla Firefox	Open	2016-12-25 00:26:16
...it.men.gov.ma	Mozilla Firefox	Open	2016-12-25 00:26:16
...angle.ma	Mozilla Firefox	Open	2016-12-25 00:26:16
...54@update-academy.com	Mozilla Firefox	Open	2016-12-25 00:26:16
...e3@www.forlife-shop.com	Mozilla Firefox	Open	2016-12-25 00:26:16
...ney.is	Mozilla Firefox	Open	2016-12-25 00:26:16
...arket1.com	Mozilla Firefox	Open	2016-12-25 00:26:16
...tstomarket1.com	Mozilla Firefox	Open	2016-12-25 00:26:16
...A6kCz@payeer.com	Mozilla Firefox	Open	2016-12-25 00:26:16

Figure I: Vulnerable websites as per Loki

Conclusion

Our detailed Labs blog post about “[When Scriptlets Attack](#)” shows how organisations with a low BIQ suffer from extended compromise dwell time (in this case 12 days), inefficient resource usage, unnecessary expenditure of analyst and responder time to correctly triage the threat (approximately 20 man hours), and exposure to a secondary attack vector of file-less attack using unchanged credentials to gain unauthorised access.

If you have a high BIQ, informed by malware behavioural analytics, the breach is not inevitable. Seeing each specific activity engineered into a file makes it immediately obvious when an encounter is malicious. Better security is not just about prevention. The scriptlet and Loki attack demonstrate how Behavioral intelligence with visibility of the real capabilities of the attack makes it possible to detect the attack and implement mitigation efforts on day one instead of waiting until day 12 when it finally is recognized by a critical mass of AV tools and untold credentials have already been stolen.