Signed, Sealed, and Delivered – Signed XLL File Delivers Buer Loader

fortinet.com/blog/threat-research/signed-sealed-and-delivered-signed-xll-file-delivers-buer-loader

July 19, 2021

FortiGuard Labs Threat Research Report

Affected Platforms: Windows
Impacted Users: Any organization or individual
Impact: Remote attackers gain control of the vulnerable systems
Severity Level: Moderate

Introduction - Signed XLL File Delivers Buer Loader

FortiGuard Labs has discovered a malicious spam campaign that uses the names of two well-known corporate entities as a social engineering lure to trick a target into opening a maliciously crafted Microsoft Excel document. When opened, the document contacts a remote server that downloads a malicious payload from a predefined website. What makes this campaign different from similar malicious spam campaigns is the use of a signed Microsoft Excel file with an .XLL file extension, rather than the standard .XLS file extension.

In this blog, we will examine details of this attack as well as the infrastructure they used. The reader will see the multi-step process used to ensure that the target would be infected, including evasive steps to bypass detection technologies via the .XLL file extension and the use of a valid signed digital certificate.

What Exactly is an XLL File Extension?

An XLL file extension is used by Excel Add-in files to allow third party applications to add extra functionality to Excel. XLL files are similar in structure to DLL files. They allow for calls of specific Excel commands, worksheet functions from Visual Basic (VBA), registered XLL commands, and *from* functions referenced in Excel. The use of XLL files is not as common as a maliciously crafted XLS file that contain macros or exploits, so it is a rarely observed evasion tactic used by threat actors to bypass endpoint detection.

Complicating things even further, the malicious XLL file used in this campaign (at the time of analysis) is signed with a valid digital signature and chained accordingly. Signed malware containing valid digital certificates are used by threat actors to evade detection as they are trusted by antivirus and other endpoint security software. Because a company or organization is vetted by a certificate authority (CA) before the issuance of a digital certificate, operating systems and anti-virus software treat files signed with these certificates as clean, which ultimately allows the signed file to operate with impunity.

And finally, when run, the maliciously crafted Excel file connects to a predetermined server to download the payload, which in this case is Buer Loader.

Campaign Details

The modus operandi of these attackers is spam email. Based on our observations, these attacks do not appear to be targeted, but instead appear to be blanketed campaigns looking for low hanging fruit—i.e., anyone willing to open the malicious attachment.

The email in the example below is a variant of the classic shipment courier status email, with this variation using DHL and Amazon trademarks as the lure. This specific example was sent to an individual and not to an organization, further reinforcing the idea that these campaigns are not targeted.

This malicious spam appears to be rushed or the product of non-native English speakers as there are grammatical issues—“We sincerely sorry due to inconvenience...”—which makes it less than convincing, even to the untrained observer.

Figure 1. Email sent to recipient with malicious attachment

(Incidentally, the recipient of this particular email has had their email username and password posted online previously. And according to haveibeenpwned[.]com, this email address has also been exposed in four separate breaches.)

Contained within the email is an attachment with the file name "Detailed Invoice.xll." Looking at the attachment we can see that it is digitally signed and chains appropriately. The digital signature is assigned to HORUM, with a reference email address of admin[@]khorum[.]ru:

Figure 2. Digital Signature Details

The certificate appears to be valid until 3/24/2022:

Figure 3. Certificate Details

Visiting the website directly offers no further details as to what entity is behind this campaign:

Figure 4. Khorum.ru showing empty directory

Same with the WHOIS information:

Figure 5. Korum.ru WHOIS details

The Infection Chain

When the user opens the XLL file, the Excel file triggers on xlAutoOpen in a similar fashion to a macro. The following image shows the export name is the same.

Figure 6. Export name same as Excel command

The export attempts to contact the following URL:

hxxp://dmequest[.]com/dme/images/portfolio/products/1/csrsc.exe hosted on 68[.]67.75.66.

Analysis reveals that the IP address serving the executable file belongs to a webhosting reseller in Florida in the United States. Further analysis shows that this is most likely a compromised server and, based on experience, it is probably controlled by affiliates of the bad actors or the bad actors themselves.

Taking a deeper inspection of the server we see that it contains an open directory that is public. In the folder where csrsc.exe resides, a directory timestamp appears to have been changed to look like it is one of the original files from 2016. However, analysis revealed that the csrsc.exe file was actually compiled in 2021.

Figure 7. Readable directory

The directory also contains several other files from June 2021 that may be from a different campaign. We have also observed older campaigns over the past several years being downloaded from this same IP address. Some of these campaigns involve serving fake data recovery software as well as PayPal themed phishing sites. However, it is difficult to determine if these attackers are all related, or if this is simply a leased server used by multiple threat actors.

A passive DNS entry of domains that resolved to this IP address highlights a variety of businesses entities, but overall, they appear to be a random collection of websites of customers belonging to the webhosting reseller.

Once the XLL file finishes downloading csrsc.exe, the downloaded file is saved as:

%PUBLIC%\srtherhaeth[.]eXe

Further Insight into srtherhaeth.exe

The downloaded file is Buer Loader. First discovered in 2019, Buer Loader is Malware-as-a-Service that was first used by threat actors to deliver banking Trojans and various other malware. As it gained popularity it was later adopted by Ryuk threat actors to help establish an initial foothold on targeted networks. Once this foothold was established, the infamous Ryuk ransomware was then deployed. Buer Loader has evolved since then and the following provides further insight into this latest version.

Analysis of srtherhaeth.exe reveals what is likely an invalid or expired signature, and because of this it did not chain appropriately and could not be verified as a legitimate certificate.

Figure 8. Invalid Digital Signature

Figure 9. Invalid Certificate

Further examination of the file revealed the following:

File Version Information

Copyright Cistae

Description Weenong

Original Name Detrition

Internal Name Phytoflagellata

File Version 0, 1, 3, 1

Comments Nonrival

Date signed 2010-09-08 00:04:00

RUST Crates and Toolchains

srtherhaeth.eXe is almost 2 MB. In the world of malware, files in this size range are not common. This is a newer variant of Buer loader that has been completely rewritten, as first pointed out by ProofPoint in May of 2021. A deeper dive reveals that it was written in RUST and uses RUST crates/libraries, which explains the file size anomaly versus traditional malware.

Consistent with the latest version of Buer Loader, this version was observed incorporating the whoami (https://github.com/libcala/whoami) RUST crate, which allows for details such as current user info including username, full name, preferred language, OS name/version, and environment it is located in. The version used is whoami-1.1.1, which was released on 2021-03-13 (https://github.com/libcala/whoami/blob/main/CHANGELOG.md)

One interesting component of RUST are toolchains. In layman's terms, RUST toolchains are collections of programs along with multiple dependencies needed to compile a RUST application.

RUST toolchains observed used so far by Buer were:

ureq 2.0.2

> A minimal HTTP request library

minreq

- A simple, minimal-dependency HTTP client with less features than ureq.
- A user-agent string of “something/1.0.0”

Ring

> According to the official site, Ring is a safe, fast, small crypto focused on general-purpose cryptography. It uses RUST with BoringSSL's cryptography primitives.

Finally, the file receives additional instructions from its command and control (C2) server:

hxxps://shipmentofficedepot[.]com (195[.]123.234.11).

Insight into C2 shipmentofficedepot[.]com. (195[.]123.234.11)

Detailed analysis over a 30-day period revealed a large majority of connections from US-based victims (66%), followed, interestingly enough, by Mozambique (22%), Singapore (5%), and other countries at (1% or less).

Figure 10. All traffic to 195[.]123.234.11 over a 30-day period

A cursory review of our telemetry indicates that over 1/3 of the traffic occurred over port 22 (SSH/SFTP). Almost all of these port 22 connections originate from a reportedly compromised server. Since this is a shared server hosting multiple websites, this information indicates that the provider may not mind hosting malicious websites.

Conclusion

While the use of malicious XLL files is not new, it is rarely used. But couple that with the fact that a valid digital signature was used (at the time of the attack) and the level of sophistication and resourcefulness of these attackers increases in the minds of threat researchers. Even though the email lure used was basic, this may only indicate that the group behind this campaign was simply testing the effectiveness of their techniques.

However, the techniques used in this campaign are harder to spot than the average attack. The examples in this blog highlight a carefully thought-out campaign by the attacker, who took the needed time and steps to ensure that their work would not be detected before infection. Thankfully, Fortinet customers running the latest definition sets are already protected against this campaign.

Fortinet Protections

FortiGuard Labs has **AV** coverage for the samples mentioned in this blog as:

W32/Agent.ADBL!tr
W32/Buerak.TO!tr.dldr
W32/Kryptik.HLHY!tr
W32/PossibleThreat

All known network IOCs are blocked by the **WebFiltering** client.

All known IOCs are blocked by **FortiEDR's** advanced real-time protection and have already been added to our cloud intelligence to prevent further execution on customer systems.

FortiMail, powered by threat intelligence from **FortiGuard Labs**, can detect and block phishing attacks and remove or neutralize malicious attachments

Fortinet's Phishing Simulation Service, **FortiPhish**, can also be used to proactively test the susceptibility of your organization to these kinds of phishing attacks.

We also suggest that our readers go through Fortinet's free **NSE Training**: NSE 1—Information Security Awareness, which has a module on Internet threats designed to help end users learn how to identify and protect themselves from phishing attacks.

IOCs

Detailed Invoice.xll

6F9D943F88F715FF8A122D7B88AF986C1A9F38F4484E48CDE768CF22A5935EFE

srtherhaeth.eXe (Buer Loader)

C28ABAAAD1B7B2C7A37F28E974E8214F07C88FEFFEF986E0A60A44AB0FA575AA

Payload Download URI

hxxp://dmequest[.]com/dme/images/portfolio/products/1/csrsc.exe

C2

195[.]123.234.11

Additional Buer Loader (contacts 195[.]123.234.11)

bd734170160b363e70602626baab37a1eb93cfb2d254cf17b6ff1b5e7313b568

9d1be741e3b09057cdaffb6e87d602afff496dee364767b161dfaab7e639866d

MITRE ATT&CK

Initial Access

T1566.001 – Spearphishing Attachment

Execution

T1204.002 – Malicious File

Persistence

T1547.001 – Registry Run Keys / Startup Folder

Defense Evasion

T1218 – Signed Binary Proxy Execution

T1480.001 – Environmental Keying

T1497.001 – System Checks

T1553.002 – Code Signing

Discovery

T1082 – System Information Discovery

T1497.001 – System Checks

Collection

T1005 – Data from Local System

Command and Control

T1071.001 – Web Protocols

T1105 – Ingress Tool Transfer

Exfiltration

T1041 – Exfiltration Over C2 channel

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.

Learn more about Fortinet's free cybersecurity training, an initiative of Fortinet's Training Advancement Agenda (TAA), or about the Fortinet Network Security Expert program, Security Academy program, and Veterans program. Learn more about FortiGuard Labs global threat intelligence and research and the FortiGuard Security Subscriptions and Services portfolio.