Fake Purchase Order Used to Deliver Agent Tesla

fortinet.com/blog/threat-research/fake-purchase-order-used-to-deliver-agent-tesla

March 7, 2022

Since the dawn of phishing, fraudulent invoicing and purchasing schemes have been one of the most common lures. The usual modus operandi involves appealing to the recipient's desire to avoid incurring a debt, especially where a business may be involved.

FortiGuard Labs recently came across an interesting phishing e-mail masquerading as a purchase order addressed to a Ukrainian manufacturing organization that deals with raw materials and chemicals. The e-mail contained a PowerPoint attachment that is in reality a sophisticated, multi-stage effort to deploy the Agent Tesla RAT (Remote Access Trojan).

What makes this campaign unique is the usage of PPAM, which is a file format that is not very common. A PPAM is a Microsoft PowerPoint add-in that gives developers extra functionality, such as extra commands, custom macros, and new tools. This blog will detail the infection process and subsequent malware deployment.

Affected Platforms: Windows
Impacted Users: Windows users
Impact: Compromised machines are under the control of the threat actor

Severity Level: Medium

Examining the phishing e-mail

Like so many computer-based attacks, this one began as a phishing e-mail sent to an organization in Ukraine.

Figure 1. E-mail to the target recipient.

Spelling and grammar issues aside, like most good phishing campaigns this one provides a time sensitive statement urging the recipient to urgently review the attached order.

Looking deeper at the e-mail and where it came from, we can see some additional information in the headers.

Figure 2. E-mail headers showing the origin of the message.

Figure 2b. Parked page.

The e-mail originated at an address of *194[.]99[.]46[.]38* that corresponds to *slot0.warongsoto.com*. This is hosted on a run-of-the-mill VPS server. Visiting the server, we noticed that the site states that the server control panel is controlled by VESTA. Recent CVE data highlights that Vesta Control Panel is affected by remote command execution and elevation of privilege vulnerabilities that ultimately allow for full compromise of the system (CVE-2020-10786 and CVE-2020-10787).

The domain itself appears to be either abandoned or at least unused with no active content hosted. It was registered in the United States in October 2021.

The originating e-mail address does not appear to reference an actual individual and a search for other instances of this being used elsewhere came up empty.

Examining the dropper – stage 1

Phase 1

Dropping the final payload occurs in multiple phases, making this, in actuality, a very complex operation. As shown in *Figure 1*, attached to the e-mail is the file “order001.ppam”. This is an add-in file format used by Microsoft PowerPoint that, in this case, contains a malicious macro that acts as a dropper for Agent Tesla.

The first phase of stage 1 begins with opening the PPAM attachment to activate the macro contained within.

Figure 3. Visual Basic macro contained within “order001.ppam”.

Once the macro is executed, it will reach out to the URL shortener Bit.ly to download the next phase of the dropper. The address used is: hXXp://www[.]bitly[.]com/awnycnxbcxncbrpopor/

Phase 2

The call out to Bitly will be redirected to a location on MediaFire – a file hosting site (hXXp://download2261[.]mediafire[.]com/6lcqxbws032g/wctsdmx4dsh95xs/19.htm). As possibly inferred, this was a campaign and not simply directed at one recipient. There were multiple files made available over several days, as shown below in *Figure 4.*

Figure 4. MediaFire repository showing multiple other files from this campaign.

Each of the files is very similar (with minor tweaks) to the download location of the next step. *Figure 5,* below, shows 19.htm as it appears if downloaded directly.

Figure 5. HTM file as it appears when downloaded.

If we arrange the file into a more readable format, we get a better sense of what it's trying to do.

Figure 6. Key part of the HTM file.

As seen in *Figure 6*, the file attempts to *taskkill* several applications and services followed by adding a scheduled task into the Windows Task scheduler. The script then attempts to download and execute another file from MediaFire - hXXp://www[.]mediafire[.]com/file/otza6n31talvvle/19.dll.

Phase 3

While the file extension gives the impression of a Microsoft *dynamic link library* (.dll), 19.dll is in actuality a PowerShell script containing instructions in a large amount of hexadecimal data.

Figure 7. HTM file as it appears when downloaded.

Once executed, the hexadecimal data will be transformed into additional PowerShell commands that will run in memory. For example, new registry keys will be added to assist with persistence.

Figure 8. Added entries to the Windows Registry.

If captured and reviewed, the entries that stand out the most are two large, compressed byte arrays — $nona and $STRDYFUGIHUYTYRTESRDYUGIRI.

Figure 9. Large byte arrays.

As can be seen in *Figure 9*, the byte arrays are then decompressed for use. Once decompressed, these can be saved as executable Windows files. $nona is the larger of the two and is Agent Tesla. $STRDYFUGIHUYTYRTESRDYUGIRI will inject Agent Tesla into a running Windows process.

Renaming 19.dll to 19.ps1 allows it to be executed as a normal PowerShell script. With this particular sample, it will attempt to launch and then inject Agent Tesla into the aspnet_compiler.exe application.

Figure 10. On the left, the PowerShell script can be seen to be launching aspnet_compiler.exe

Examining the malware – stage 2

At its core, Agent Tesla is a keylogger and RAT (Remote Access Trojan). It will take any results captured from the keyboard and clipboard and send them back to its C2 (Command and Control) server. In this instance, once injected into the aspnet_compiler.exe process Agent Tesla will be up and running. With entries in the registry it will have persistence to run even if the host machine is rebooted.

Figure 11. Agent Tesla running inside a debugger.

As can be seen in Figure 11, this variant is similar to one FortiGuard Labs has analyzed previously.

From this point, it will run in the background and observe the user, recording their actions and sending them back to the threat actor.

Figure 12. Typical connection cycle to Agent Tesla's C2.

Conclusion

Threat actors for the most part like to use lures that are tried and true, as was the case here with the invoicing phishing e-mail, because they continue to enjoy success. The dropper attached to the phishing e-mail shows the continuing evolution and complexity required to evade modern security controls combined with the need to traverse several gates to arrive at the release point for the final payload.

Once finally deployed to a system, the ability to obfuscate and hide inside everyday files and processes proves that Agent Tesla is a very capable and formidable threat. Unfortunately, this trend towards increasing sophistication is unlikely to abate any time soon.

Fortinet Protections

FortiMail's integrated antivirus, sandbox, and content disarm and reconstruction (CDR) functions detect and disable this malicious attachment. The FortiGuard Antivirus service detects and blocks this threat as:

- VBA/Agent.GBX!tr
- JS/Agent.YHB!tr
- PossibleThreat.PALLAS.H

The domain warongsoto.com is blocked by the Web Filtering client.

IOCs

Sample SHA-256:

DLL/PS1 SHA256
27C7F5F2A21298C66A8EEF11DF73BFB1E9EEF7B84974CEF9AF695A7E216EFA21
F86FDC385BA4467FD27093DFB6A642C705199AC3307D24096D7150FB6A80E8FD
9971EE4C59F1838C111CFAA0BC26A6C08B80FD7364C193F6D8DCA1A840D37B7F
D147E24E603FB17CE3C6EC839CC8AD07BCE06455037CC0E139CC68042153B7A7
7659EC63CF7010158517AD0DFD3828F8B46592BDBC374D906BACD80A8500DA4B

D98D56AEB0A3DBD020C1F6ED9CFE0848A4D8C57DABBB064FBCD0305BDF8B329C

4FD01BF61C49579A40EFDD86D736930585AB3E79D9085177303DDCFF61480E26

7384900E7BB02B1028D92A145CBE2BDB5E3283336C0E5E6014AFCD546B17B985

EFDFD9CCDFB052FD7693403D1E8E085594C1B3B7ED221FD6021F794B5BA752C5

90313F269F0583FBC179BEABAE2A48B1B53594F1FB4A27556861D5D82AD722EC

3C1636CF2A4296840D55A8BAF9ABB56E1C847C5D6E3A7DF0D7040050D017E54C

EC9E8CB17C92C4D6175FB3E715F73C4BEF833742168451398A99DE22F06FB52E

87B7F2C05F3E63821DE8AD22EE7ED9CA034CD61332EBAE3E1F76AF085696D5F8

B5CF3D2594E148C458467C833B0D95976480FB054A7763E1F6DCF4187A61E1BE

0C3F881258EF9F1DB9A9923945AB07351DA8BA1A337AACCBCB6B5BD56AE080B3

3B9D6FC6449B7B42E816A19C2B649A5E5CF4E724B2FCD93E56445DECA89FB850

34CFFA6664C92F77EE60749E251A4ED18A15A3F0F61C78BCADA9EA86478681E0

380C8FC86237A6B847F40870E9A15ADA1914F25174FF40838604354389EF9540

B8403149F7A6E0FCCCB9C6E793BDCE7431385F86174D80B0C65F89A9C948A47F

D7E76887903EBD361112531017E140D2BFAAA816598C648F3B1238DCC6906BF1

CB758A93876ACD5F7A314FDA6CCB97D0FC115ABFFF7F22637B629B1E91CF1970

F3D9873EE798BF649A22C50E3DAEEBADFC127A405C0D8F54266B66C4377901E0

1BD2383346BF8B1924C179B1616AF56A2BC4248717329B90E01FF13DB45ABE4F

5DC6B8CC1E9D1EE535752E6C5320280F864EA660B5BF8657F96B8E2B1053C57A

FA37BD017B82C1F7C545475F7A0CD786F81BC2CC024DA46CBDB4071B22ED4FFB

Fileless Tesla SHA256
F69B85F5763CEC5A5DA5CE1152038FFEEF7A2A75600003ADBFEB3DC87502C8A8
B409FF4CD1B8F18E80AFA98B3306440391FB5CBE294E6DA14E8146F63ECA2C6C
34EEEDAB0ABBEB1BAFFCCFDAEF74E54A7786F24BC5024B2F23A6F9385FEC9917
6449D03A519CAB4B7C4E19D53D57A16AE69B70D7DF6BE815BCB57DC7395AB991
E77DCCCB70AD61D50AC7E8C5DA1F79D5BC22B1F42A6651252EB449241BD6068B
C7840150DC084B1E0F6961EC61C39793BBED40FE17A7E24124DFE07F2C1A7B40
F4542569E3F54CBC93AB835567507242DDDCAE2A84743DA103332EEFF3501ABD
851CC3973B096C8DA88E1EDB568C17750D019CA7F2528B3DA933D33D7F306A46
C0C3A9CBDC769F3B86EAB40A9032769FE61E5E9B93CE7A93A0CC02EF43D4B9B5
256F7CC33E3E359427702FF79E59C5EEA73164CC74D96B6F24E6BE19B62500E7
445E6D6EBA924CC86005C107F329B248997AAC4149FBBD540A656FBA50A68C19
D321AF1AF7D8B0A19B87897938B23ADB57C9089B73F2C15E0E2747B0071D1715
822F2266CA284C5318E75C1286F7B4ED746E9289323B57462E227ED8D4D1AC8F
399B6B1AED4B62C165FE074DD9A43DEC0F0E1D5A50C89BFCA4A902CBFDBC17D5
6BCDC49281217C3D8A82ED29A6BC89154885B08954AC3F78FA11BB09BF34A109
1DF27F8D8B8572CB76D7275D7FE686C88F4297DA39095C1399B1E55459DFFDF6
49BF5F9D59C27291FCB0D9F0C593DCB00CA9705E5D294E9C55353BDEFBC37273
A155AB7DB6D22A44487D909BB040F5300B6E24283CDB7D7D902E7CE5CDD533BB
FD210DFB8C2F3B33FEEE191608EF58DD2816F08E9850DB734143115BA199690E

5F53A249455BB903C2C57A5CE23BFA6D069966034F74947A70037DEB1459DC88
AD3BE25985B1DFA0A72C7CE59365F2AE7142FB4B2A78B7905D10AEB13998DDD4
9783473EFECA3003D6A1B8DB8FE0E1A8AA291F170110D974C058806A25B4C419
B1043F48E99EF5B98F4987E1FFD3200CD6A32B3427BA2762310FDEA58934D95C
3E99AA348FAFFDF2D73867C47067EA17A96CA36E5329E30C3A37F45B4274D165
0ABBD4F17EC6DEDEFA188E39501B923286C56627ACB87FEC73271E459A383D0D

Filename	SHA256
Order001.ppam	DCA3AC723A130E56FB158C34C68E1C4B7D8577D0DBE9D8B859BFFF7ADA34D02E
Loader	4C0E2CB721585C480169B3804E17E2761BC5FE76584CF1375FCCDB33CA64D5A5

Network IOCs:

192[.]154[.]226[.]47
hxxps://www[.]mediafire[.]com/file/s2w0i5rhl9e4wje/1.dll
hxxps://www[.]mediafire[.]com/file/u8t0g2vyrvoyldp/10.dll
hxxps://www[.]mediafire[.]com/file/hheln09oi15b266/11.dll
hxxps://www[.]mediafire[.]com/file/mra2u90srnmymxl/12.dll
hxxps://www[.]mediafire[.]com/file/e7fmuc053m1vdz5/13.dll
hxxps://www[.]mediafire[.]com/file/l3xh5g98wf5l4gv/14.dll
hxxps://www[.]mediafire[.]com/file/5d7sd1qat59dtpy/15.dll
hxxps://www[.]mediafire[.]com/file/2tpkh278oypz794/16.dll
hxxps://www[.]mediafire[.]com/file/hjjo0rc7izwy4is/17.dll

hxxps://www[.]mediafire[.]com/file/wy0e3mn2xyaqdhd/18.dll
hxxps://www[.]mediafire[.]com/file/otza6n31talvvle/19.dll
hxxps://www[.]mediafire[.]com/file/dsgxrjtpbyyzm7u/2.dll
hxxps://www[.]mediafire[.]com/file/mf3pufkmdshddyq/20.dll
hxxps://www[.]mediafire[.]com/file/ijdnf0wqv4e5frr/21.dll
hxxps://www[.]mediafire[.]com/file/c9gt9xi3l9srlhi/22.dll
hxxps://www[.]mediafire[.]com/file/pqk7p5p1vvcv5s1/23.dll
hxxps://www[.]mediafire[.]com/file/mqbl43fcem1fndd/24.dll
hxxps://www[.]mediafire[.]com/file/xz0guzs3g004f0i/25.dll
hxxps://www[.]mediafire[.]com/file/qe4ece114vu4n0o/3.dll
hxxps://www[.]mediafire[.]com/file/wbh1kq3u82mcso6/4.dll
hxxps://www[.]mediafire[.]com/file/x0o4nlef7snbixu/5.dll
hxxps://www[.]mediafire[.]com/file/xrnlyn4pjcmcfyf/6.dll
hxxps://www[.]mediafire[.]com/file/qbzdrs7ulvvzfay/7.dll
hxxps://www[.]mediafire[.]com/file/9q41qxg988c3opx/8.dll
hxxps://www[.]mediafire[.]com/file/xxbskabqkber6oq/9.dll

Mitre TTPs

Resource Development	
Stage Capabilities: Upload Malware	T1608.001
Initial Access	

Phishing: Spearphishing Attachment	T1566.001
Execution	
Command and Scripting Interpreter: PowerShell	T1059.001
User Execution: Malicious File	T1204.002
Persistence	
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
Defense Evasion	
Process Injection: Portable Executable Injection	T1055.002
Reflective Code Loading	T1620
Credentials Access	
Credentials from Password Stores: Credentials from Web Browsers	T1555.003
Input Capture: Keylogging	T1056.001
Discovery	
Account Discovery	T1087
Command and Control	
Application Layer Protocol: Web Protocols	T1071.001

Thanks to Val Saengphaibul who helped contribute to this blog.

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