Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

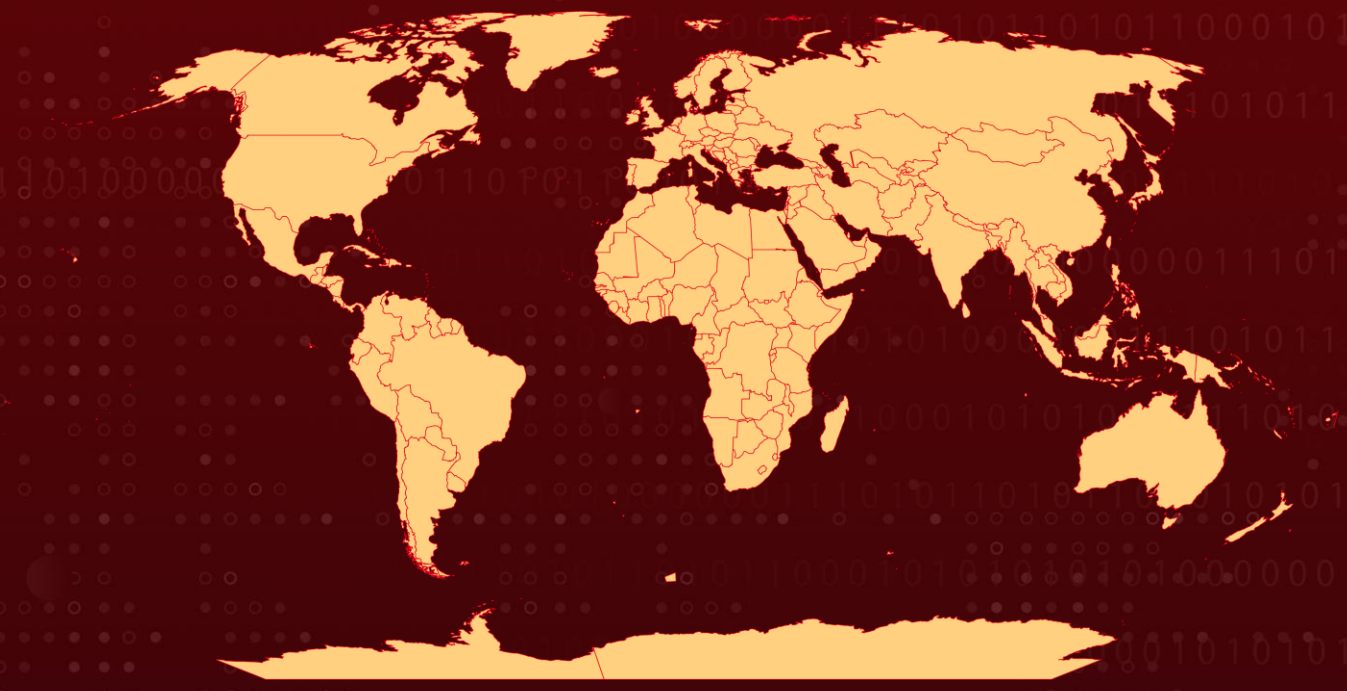
Agent Tesla's New Variant Spreads Through Crafted Excel Files

Date of Publication	Last Update Date	Admiralty Code	TA Number
September 7, 2023	December 20, 2023	A1	TA2023359

Summary

Attack Began: August 2023
Malware: Agent Tesla
Affected platforms: Microsoft Windows
Attack Region: Worldwide
Attack: A phishing campaign has surfaced, disseminating a new iteration of the Agent Tesla malware through a meticulously crafted Microsoft Excel document. This document exploits a longstanding memory corruption vulnerability within Microsoft Office's Equation Editor, dating back six years.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✗	✓	✓
CVE-2018-0802	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✓	✓	✓

Attack Details

#1 A novel iteration of the Agent Tesla malware lineage has surfaced within a phishing campaign, utilizing a meticulously crafted Microsoft Excel document as its attack vector. This malware exploits two distinct vulnerabilities: CVE-2017-11882, a memory corruption exploit within Microsoft Office's Equation Editor with a six-year history, and CVE-2018-0802, enabling the download and execution of the Agent Tesla file on the victim's device.

#2 Agent Tesla possesses comprehensive data exfiltration capabilities, enabling it to extract sensitive information, including credentials, keystrokes, and screenshots, from compromised devices. The initial breach in this phishing campaign occurs when a malicious email attachment titled "Order 45232429.xls" is transmitted.

#3 This attachment, in OLE format, conceals intricately crafted equation data that exploits the long-standing CVE-2017-11882 security vulnerability. This vulnerability triggers memory corruption within the EQNEDT32.EXE process, allowing for arbitrary code execution through the Process Hollowing technique. In this method, a malicious actor replaces the original code of the executable file with malicious code.

#4 To ensure persistence, Agent Tesla employs two distinct methods, even when the device undergoes a restart, or the malware process is terminated. The first method involves executing a command to create a task within the Task Scheduler system, which is embedded within the payload module. The second method adds an auto-run item to the system registry.

#5 For transmitting pilfered data, Agent Tesla offers a range of options, including the use of the HTTP POST method or embedding the data within the body of an email sent via SMTP. In the case of this variant, the stolen data collected from the victim's device is transmitted using the SMTP protocol for email delivery.

Recommendations

Regular Software Updates: Ensure that all software, especially Microsoft Office and its components, are kept up to date with the latest security **patches** and updates. This helps in mitigating vulnerabilities like CVE-2017-11882 and CVE-2018-0802.

Network Segmentation: By implementing a strong network segmentation strategy and isolating critical systems, the lateral movement of Agent Tesla malware is effectively restricted. This proactive approach significantly reduces the risk of malware spreading within the network, offering protection against threats like Agent Tesla.

Behavior-Based Intrusion Detection: Consider implementing behavior-based intrusion detection systems that can identify anomalous patterns and activities, even if they involve novel malware strains. This can provide an extra layer of defense against Agent Tesla's innovative tactics.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1566 Phishing	T1566.001 Spearphishing Attachment	T1059.005 Visual Basic	T1137 Office Application Startup
T1574.002 DLL Side-Loading	T1055.011 Extra Window Memory Injection	T1027 Obfuscated Files or Information	T1036 Masquerading
T1112 Modify Registry	T1497 Virtualization/Sandbox Evasion	T1562.001 Disable or Modify Tools	T1564 Hide Artifacts
T1018 Remote System Discovery	T1057 Process Discovery	T1082 System Information Discovery	T1083 File and Directory Discovery
T1518.001 Security Software Discovery	T1071 Application Layer Protocol	T1105 Ingress Tool Transfer	T1203 Exploitation for Client Execution
T1056.001 Keylogging			

Indicators of Compromise (IOCs)

TYPE	VALUE
File Names	Order 45232429.xls, dasHost.exe, nicko.vbs, nix.txt, knog.txt
URLs	hxxp://23[.]95.128.195/3355/chromium[.]exe, api.telegram[.]org/bot6362373796:AAFAjB2uG5ePhAcUiHforF23Ij_H_LDLFUs, api.telegram[.]org/bot6475150763:AAFSaMWIpAeiCNQFdS0vxz0W6HCxWx96MFk/sendDocument, api.telegram[.]org/bot6663697988:AAHBsfmbPr_JinYR7jDRpZloxUBi6EcQ6HE/sendDocument
SHA256	fdc04dc72884f54a4e553b662f1f186697daf14ef8a2dc367bc584d904c22638, 36b17c4534e34b6b22728db194292b504cf492ef8ae91f9dda7702820efcfc3a
SHA1	e2437078fe7f3abd635dacae65cf6ae2d10ef98e
IPv4	79.110.48[.]52, 79.110.48[.]52, 193.42.33.51
MD5	c1ac31ebcbfb8dc95d4eea6d4c95a474, 201cd0a2fc6a87d25d6aed1e975fae71, 38f6b4d5804de785b925eb46ddd86d6f, c1521547dea051bd7a007516511fb2ca, dddabc8019a7184055301927239a9438, f302addf3b4068888788d8edce8f52a0, 1402e4408f123da1e9bc3bde078764fc, a1c2b285a7ff9dd99c70e4d750efea51, 8496654930be3db6cea0ba62ffe5add9, d6f8c9a88cbdd876695f4bef56972f2e, 8d17b59e8bb573b12a9d0e42746f8aef, 8955b482e59894864bace732302a9927, f5f51251dc672e1934746e0057011b1a, 5630282a95afd2a5ceeecc5acf7ff053, 547b88c4aa225377d7d65e912d81fe28, 87aa9fc1bf49d48234160a15515a8145, 0ada110f82ce64fcfab0eb0e5d8d948e, 32e9af7d07a5edcc9bf9b5c8121acc55, b551da554933c2c064f96aaa6aa9ff55, 7ea06a0e6c1e5707a23364ae6984b4f3,

TYPE	VALUE
MD5	f3f27883dc91a7c85a03342bf6fed475, 7c9ad2b73748f8c745d5d49b9b4876c5, a8c8010963f35fc3253d6409c169a9f2, d6a1feb6cfa307c5031ea2dd2118d786, 069bb6a37f9312ba4fea6c70b7134d39, 6bdb7a11d0eaa407e7a7f34d794fb567, f11d72bc4192b2ed698cc2b0200773bf, a55302ad4bf2f050513528a2ca64ff01, 01b02fc9db22a60e8df6530a2e36a73b, 43ec3cc0836bd759260e8cf120b79a7b, 5477e3714c953df2bb3addf3bebbda9a, be1858db74162408c29c8b8484b3cf88, 38bb6b06907c6e3445aa23c8d229e542, 05bc545b9b0de1ccb4254b59961ea07b, 25a697d0e6c5fa06eea8ba0d3ae539da, 8a081a4f6c497c60c6e72dfabfe30326, ad0f5f4994a2998f0e1ed3323884837c, 092ff92d9bfa9cac81a8b892d495f42e, 09f197fc8d69ec14875723f1e6e623bf, 0eba69a4ad399db14a2743b4d68f13e8, 19eab6a97cea19473bda3010066c5990, cb2b5646d68279aea516703df3c4c1e9, 3247ad04996dd2966800153e7ea14571, 92d1ece422670dbf9a3e1aef45612b5c, f25da7cd5fb33e7a0967dbcdf008bd9a, a7f2d131a2f3f61978ec17395f7b34b1, 39088a9e4ad3e7a8ba4686641569dbcd, 210e9a89b723b3246a7d590c9a428c83, efc3a41ecae822eba861cb88c179c80e, c01e90db99bcc939f829a181aef2c348, b18ba839dfd653b07b984330dd85b57a, a8e8d4667f96ea847d18eb7830fb1dc6, c38b8d525f48cbdf92381274059d8f0b, 6e0dafacdeee6f2d9463d0052db5cce8, b6f892c73fa0f491072592d7baf0c916, bf9d9c9a95fdb861c583dc9b66bcf5ab, 0043f65755a700b94a57118a672df82c, adbf1e2f49d842aac524d7ac351ca5b4, d55bdb3593664d806794d00025390081, 935e75cbd0f207bfeb6d3b5d90e35685, db4bfb57c7acd8d568a06a9c3739e146, 08e1955de35005b335be2e100d2d4a3c, e57882623add29cbfa8c93d011b52c44, e6c4636c331af09568a68dcf3614cfa4, be71e90f09a38adfe22d34e3dd044fad, e9d4e5b8b80dcb4fcf5af8413066434e,

TYPE	VALUE
MD5	413af1ff38e6a4e205c6f487d042b457, f1a1542bbccea9a4e6746040d85eae1b, 05d60c7be299fc0220ffcaf3b1482652, 5373b6dce20bbb0218034aa9bf0c20df, 1e22cd428f5baf23877a8189469ed92a, b76d8d59b53f58dd876951044e6d88b9, a29585da474f79a723894c1a56f65b85, 2639c8b09f744e95ba612c89ef26e02c, bba5761789159b5a1a23566506358c15, 3d8414800762efb9276a999fc477211b, f0af137175487b4d1249921ce506efe9, 2123f750f5b854b439349576118d9b9d, 7b6ec969d4110722b427de45ca1c0d42, 6dfc461ecf4f2fe4c5f44cdeb6792226, 0708c52198a49bc7ab16bce19472598a, 00b28f548f14de4f53abd6651bf78b98, ea1472bad426efded678a15c9a14bf34, dadb38b97d45d7438fbd43911a71d844, d7ebf4ab7bb0ab685e3902349d637e9b, aff1e141f15d808d5d4f549ea99c1e4d, bbc7c66b301d3087cfdaa89528832895, e6926fc50f40c5c5feb676b0adcb7655, 3c3580dfbc1f06636fe5696879cbdd85, b7dba4e30a73f58740d316c46645b759, 7b1bc15873c39866b429d44da8640285

Patch Link

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0802

References

https://www.fortinet.com/blog/threat-research/agent-tesla-variant-spread-by-crafted-excel-document

https://www.zscaler.com/blogs/security-research/threat-actors-exploit-cve-2017-11882-deliver-agent-tesla

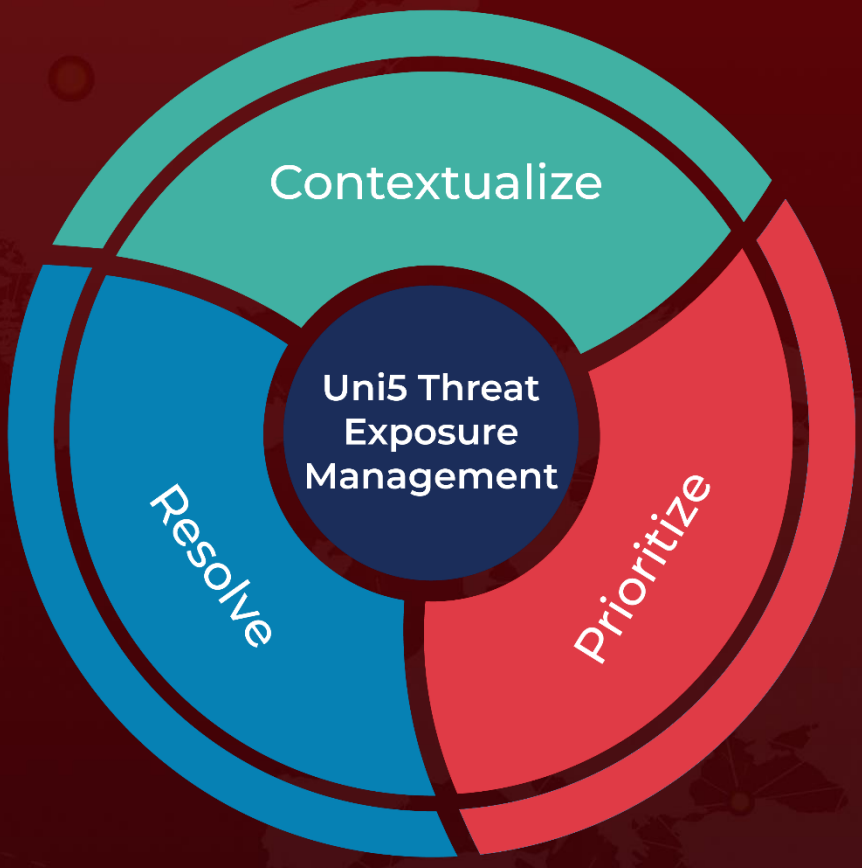
https://www.hivepro.com/agenttesla-trojan-returns-with-phishing-campaigns-using-guloader-to-steal-secrets/

https://attack.mitre.org/software/S0331/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 7, 2023 . 6:30 AM

More at www.hivepro.com