Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

MEME#4CHAN The Unconventional Phishing Campaign Spreading XWorm

Date of Publication	Admiralty Code	TA Number
May 17, 2023	A2	TA2023234

Summary

Attack began: 2023
Malware: Xworm
Attack Region: Germany
Targeted Sector: Healthcare, Manufacturing, Hospitality, and Business Entities
Attack: A persistent cyber threat known as MEME#4CHAN has emerged, characterized by an intricate phishing campaign. This cluster of malicious activity employs a distinctive attack chain methodology, successfully infiltrating targeted systems and distributing the XWorm malware.

Attack Regions

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (Follina)	Microsoft Windows	✓	✓	✓

Attack Details

#1

An ongoing MEME#4CHAN phishing campaign is utilizing an unconventional method to spread malware. The attacks are executed through code filled with English-themed memes and complex obfuscation techniques, resulting in the deployment of heavily disguised XWorm payloads that successfully infect victim systems. These attacks have been observed primarily targeting manufacturing firms and healthcare clinics located in Germany.

#2

To initiate the MEME#4CHAN attack, a phishing email is sent containing a single Microsoft Word document file named "Details for booking.docx," which utilizes the Follina vulnerability (CVE-2022-30190) instead of macros to weaponize the document and drops an obfuscated PowerShell script.

#3

Subsequently, the threat actors, believed to be English-speaking, exploit the PowerShell script to evade the Antimalware Scan Interface (AMSI), deactivate Microsoft Defender, establish persistence, and ultimately execute the .NET binary housing XWorm. Curiously, one of the variables within the PowerShell script bears the name "$CHOTAbheem," possibly alluding to Chhota Bheem, an Indian animated comedy adventure television series. Notably, the approach exhibits resemblances to the tactics employed by TA558, a threat actor previously associated with targeted attacks on the hospitality industry.

Recommendations

Strengthen Endpoint Security Measures: Organizations should bolster their endpoint security measures to mitigate the impact of MEME#4CHAN's malware payloads. This includes implementing robust antimalware solutions to detect and defend against obfuscated PowerShell scripts and the XWorm malware. Regularly updating security **patches**, especially for Microsoft products, is crucial to prevent the exploitation of known vulnerabilities, such as the Follina vulnerability (CVE-2022-30190), observed in these attacks..

Enhance Phishing Awareness and Training: Given the sophisticated and unconventional methods employed by the MEME#4CHAN phishing campaign, organizations should prioritize comprehensive phishing awareness and training programs for employees. Educate them about the risks associated with opening suspicious email attachments, emphasizing the importance of verifying email senders' legitimacy and adopting cautious behavior when interacting with unfamiliar or unexpected attachments.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment
T1204 User Execution	T1204.002 Malicious File	T1204.001 Malicious Link	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1059.003 Windows Command Shell	T1059.007 JavaScript	T1027 Obfuscated Files or Information
T1055 Process Injection	T1055.009 Proc Memory	T1620 Reflective Code Loading	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1053 Scheduled Task/Job	T1573 Encrypted Channel	T1573.001 Symmetric Cryptography
T1105 Ingress Tool Transfer	T1571 Non-Standard Port	T1041 Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f3e6621928875a322ee7230ccf186bdaa5609118c4a6d1c2f4026adfb8e88744,9cd785dbcceced90590f87734b8a3dbc066a26bd90d4e4db9a480889731b6d29,3c3e24c01a675b3b17bee9c8f560a33c3ecca8c44442fd5b3dd8c0f4429f279b,6d86f36b2220e8d9580e6708856fa74f37f7aa35db1a708e17ecacf0de3d5d2e,db1185f24c56cadec1c85a33b0efeb2d803ff00abf4c9df1e00d860683068415,41c68aecada65a15f4a8bea52cc25033a1b73ff7340cd3865d55c61ded566e81,292b5a8c61eb79633590b6b13c0b41388ccad3535b55ed822b887d6d15d61be4

TYPE	VALUE
SHA256	59d72ff91e94a2c762285cce3bcb3e94e8d14608c2eeecacdcd6fe720c3ad5f2,9419d7a578338a714f976fb2b9eb320049422ec7059cedcc4a8baf144c4df41b,2725a14da90a6bcbfde174df8b0e95179b617aa14ec07a2d1fc71000310ad913,4746941996305743c9d0bcb96ed4b2b930355cd8782098aa5600b42131314308,c443d754153180ebeee1106d5eecf1024e063413f3f92a29c6c95a08c6f2e633,1005feeff2ecfe6e53f53f63a2364de8418863d83e256322ca82e939dae95e45,6005529195e6afac29d8c62091ee7990e92b7a80b391b03c34c8a8fbf019fce6,f0942afa08c509f58b4b9f02cae4581ebf712f2f1763f1a2ffb8f9d964e335ae,d4fdc73d563605cadf1ded9b644f21e8dae0f65870890357e5bc554bbc66bf74,1b5ec95836cd52efa853ba3fa76d0849e4094b32048952a7ac0676d34f251776,1ae5589b6c358ff11a9555a7265ba5f0709be7a865e2cf51af04eb17b2a2ce18,1a517a25d55aae6af13d025b1d1edee7fb185b90155f30e195f58cbf4c6b36fe,d9a1c97646872be823bce7e37325f9869daa5593f3ced37024dc5188243639be,90cb95264d0b555fe9a760de404196ac183a958c9cc1aad0689598e35fbb0c3b,3c45a698e45b8dbb1df206dec08c8792087619e54c0c9fc0f064bd9a47a84f16,4fc40af3b2e3f96e8013a7187e5cb4ce1a00a9528823f789cb8aca09c51143c6,9a7061a539333e9f833a589197a60258ebb820bba5f1f29d5b31453e8e392d0f
IPV4:PORT	212.87.204[.]83:3000
Domain	port3000newspm.duckdns[.]org
Email Address	zoe[@]kbowlingslaw[.]com panelnew12[@]gmail.com
URLs	hxxps://73cceb63-7ecd-45e2-9eab-f8d98aab177f.usrfiles[.]com/ugd/73cceb_b5b6005e2aa74cf48cd55dca1a2ff093.docx hxxps://73cceb63-7ecd-45e2-9eab-f8d98aab177f.usrfiles[.]com/ugd/73cceb_16620dd76e094b4888c85467a58e79df.txt hxxps://73cceb63-7ecd-45e2-9eab-f8d98aab177f.usrfiles[.]com/ugd/73cceb_e5a698286daf43ac87b4544a35b1a482.txt hxxps://529f38d0-3744-4286-b484-be860d475d25.usrfiles[.]com/ugd/529f38_41875cf4c8844415994858b3623063f9.txt hxxps://42502d2a-e7ed-4a16-9f11-33ffe6c54021.usrfiles.com/ugd/42502d_fb4a2f640cf14ab2a8bcbde16bd178ba.txt hxxps://powpowpowff.blogspot[.]com/atom.xml hxxps://huskidkifklaoksikfkfijsju.blogspot[.]com/atom.xml hxxps://backuphotelall.blogspot[.]com/atom.xml

TYPE	VALUE
URLs	hxxps://3000allfitheyito.blogspot[.]com/atom.xml hxxps://urlintimacygoombguch.blogspot[.]com/atom.xml hxxps://port5000duki.blogspot[.]com/atom.xml hxxps://bakc5002.blogspot[.]com/atom.xml hxxps://billielishhui.blogspot[.]com/atom.xml hxxps://doccallingupdate.blogspot[.]com/atom.xml hxxps://urlpropogationintimitacyi[.]blogspot.com/atom.xml hxxps://www.mediafire[.]com/file/t820jnuwf9mri17/excelDNALibrary-AddIn64-packed.xll/file hxxps://www.mediafire.com/file/giv692dqvctosb3/50002023[.]txt/file hxxps://www.mediafire[.]com/file/q1zrci43zt8hlix/7000.txt/file hxxps://www.mediafire[.]com/file/79jzbqigitjp2v2

Patch Links

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

References

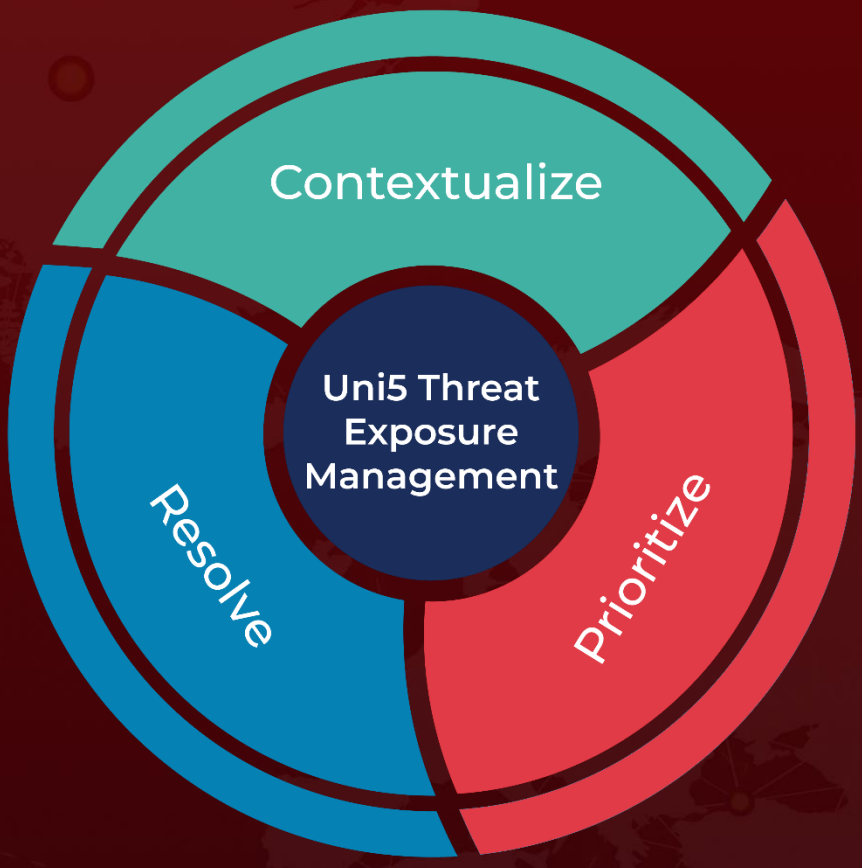
https://www.securonix.com/blog/securonix-threat-labs-security-meme4chan-advisory/

https://www.elastic.co/security-labs/attack-chain-leads-to-xworm-and-agenttesla

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

May 17, 2023 • 7:21 AM

More at www.hivepro.com