Hive Pro

Threat Level

Red

CISA: AA25-050A

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Ghost Ransomware's Brutal Reminder: Patching Isn't Optional

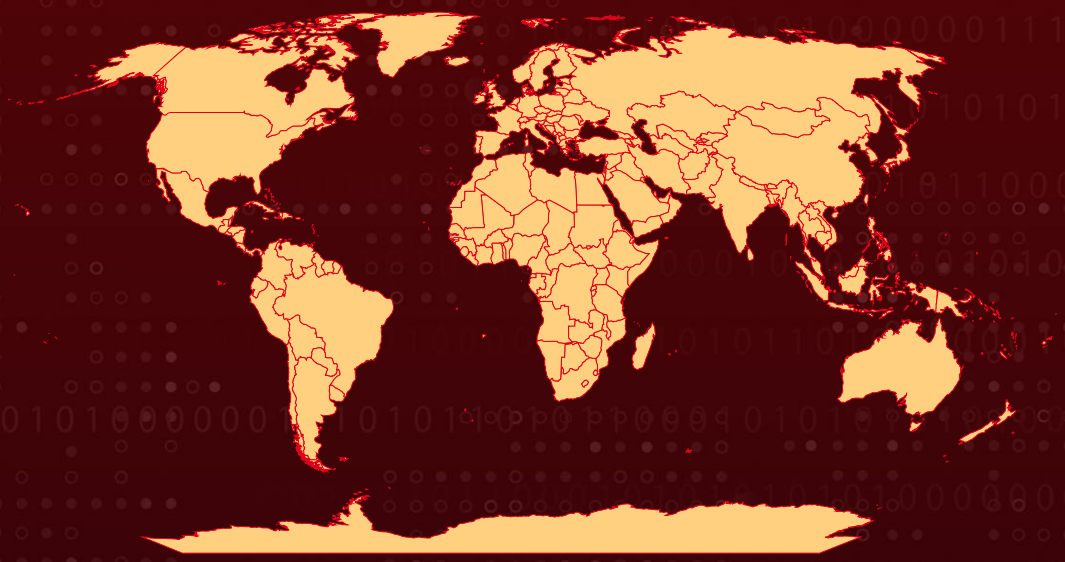
Date of Publication	Admiralty Code	TA Number
February 25, 2025	A1	TA2025057

Summary

Active Since: 2021
Malware: Ghost Ransomware
Targeted Industries: Critical Infrastructure, Healthcare, Government, Education, Technology, Manufacturing, Small and Medium-Sized Businesses, Religious Institutions
Targeted Region: Worldwide

Attack: Ghost ransomware burst onto the scene in early 2021, swiftly making headlines as it exploited unpatched vulnerabilities to infiltrate organizations across more than 70 countries, including critical infrastructure. Believed to be operating from China, Ghost's attackers showcased advanced tactics, rotating payloads, evading detection, and leveraging notorious exploits like ProxyShell to maximize impact and profit.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2018-13379	Fortinet FortiOS SSL VPN Path Traversal Vulnerability	Fortinet FortiOS	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2010-2861	Adobe ColdFusion Directory Traversal Vulnerability	Adobe ColdFusion 9.0.1 and earlier	✗	✓	✓
CVE-2009-3960	Adobe BlazeDS Information Disclosure Vulnerability	Adobe BlazeDS 3.2 and earlier	✗	✓	✓
CVE-2021-34473	PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✗	✓	✓
CVE-2021-34523	PROXYSHELL (Microsoft Exchange Server Privilege Escalation Vulnerability)	Microsoft Exchange Server	✗	✓	✓
CVE-2021-31207	PROXYSHELL (Microsoft Exchange Server Security Feature Bypass Vulnerability)	Microsoft Exchange Server	✗	✓	✓
CVE-2019-0604	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	✗	✓	✓

Attack Details

#1

Ghost ransomware first emerged in early 2021, quickly gaining notoriety by targeting vulnerable internet-facing services through the exploitation of known security flaws. Within a short period, it had compromised organizations across more than 70 countries, affecting a wide range of industries, including critical infrastructure.

#2

The group behind Ghost ransomware, believed to be operating out of China, leveraged publicly available exploit code to breach systems. Its focus was on networks where security patches had not been applied, taking advantage of well-documented vulnerabilities. Among the most frequently exploited were flaws in Fortinet FortiOS appliances (CVE-2018-13379), Adobe ColdFusion servers (CVE-2010-2861 and CVE-2009-3960), Microsoft SharePoint (CVE-2019-0604), and Microsoft Exchange (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207), commonly known as the ProxyShell attack chain.

#3 Once inside a targeted network, the Ghost actors demonstrated considerable adaptability and sophistication. They routinely altered their ransomware payloads, switched file extensions for encrypted data, modified ransom note texts, and used multiple ransom email addresses to evade attribution.

#4 This constant evolution led to the group being associated with numerous aliases, including Ghost, Cring, Crypt3r, Phantom, Strike, Hello, Wickrme, HsHarada, and Rapture. Some of the ransomware samples identified during attacks included Cring.exe, Ghost.exe, ElysiumO.exe, and Locker.exe.

#5 The attack methods employed by Ghost were highly advanced. They used Windows Management Instrumentation and encoded PowerShell commands to deploy Cobalt Strike beacons on compromised systems, enabling remote control and lateral movement. To maintain persistent access, they created new user accounts or changed passwords on existing ones.

#6 A variation of Chunk-Proxy was often deployed as a webshell, allowing the attackers to execute commands remotely and maintain a foothold within the compromised network. To avoid detection, Ghost operators disabled antivirus programs and Windows Defender, ensuring their malicious payloads could run uninterrupted.

#7 They also used credential-dumping tools like Mimikatz to extract sensitive information from Windows systems, further solidifying their control. The ransom notes left by Ghost actors typically carried a threatening message, warning victims that stolen data would be sold if the ransom was not paid.

#8 Despite these claims, there was little evidence to suggest that Ghost consistently exfiltrated large volumes of sensitive information, such as intellectual property or personally identifiable information (PII), that could cause significant harm if leaked. Their primary motive appeared to be financial gain, relying on the threat of data exposure to coerce victims into paying rather than following through on the extortion.

Recommendations

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Regularly Test Backup Restores: Conduct frequent tests to verify the integrity of backup data and ensure that restoration processes work as intended. This practice helps identify any issues before an actual data recovery scenario arises.

Prioritize Timely Patching and Updates: Regularly apply security patches to all internet-facing services and critical systems. Address known vulnerabilities exploited by Ghost ransomware, including Fortinet FortiOS (CVE-2018-13379), Adobe ColdFusion (CVE-2010-2861, CVE-2009-3960), Microsoft SharePoint (CVE-2019-0604), and Microsoft Exchange (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 – ProxyShell chain).

Network Segmentation & Zero Trust Implementation: Segment critical infrastructure to isolate sensitive data and limit lateral movement. Implement Zero Trust Network Access (ZTNA) by enforcing identity-based policies rather than traditional perimeter security.

Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0010** Exfiltration
TA0011 Command and Control	**TA0040** Impact	**T1190** Exploit Public-Facing Application	**T1047** Windows Management Instrumentation

T1059 Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.003** Windows Command Shell	**T1098** Account Manipulation
T1136 Create Account	**T1136.001** Local Account	**T1136.002** Domain Account	**T1505** Server Software Component
T1505.003 Web Shell	**T1068** Exploitation for Privilege Escalation	**T1134** Access Token Manipulation	**T1134.001** Token Impersonation/Theft
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools
T1564 Hide Artifacts	**T1564.003** Hidden Window	**T1003** OS Credential Dumping	**T1018** Remote System Discovery
T1057 Process Discovery	**T1087** Account Discovery	**T1087.002** Domain Account	**T1135** Network Share Discovery
T1518 Software Discovery	**T1518.001** Security Software Discovery	**T1041** Exfiltration Over C2 Channel	**T1567** Exfiltration Over Web Service
T1567.002 Exfiltration to Cloud Storage	**T1105** Ingress Tool Transfer	**T1132** Data Encoding	**T1132.001** Standard Encoding
T1573 Encrypted Channel	**T1486** Data Encrypted for Impact	**T1490** Inhibit System Recovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
File Name	Cring.exe, Ghost.exe, ElysiumO.exe, Locker.exe, iex.txt, pro.txt,

TYPE	VALUE
File Name	x86.log, sp.txt, main.txt, isx.txt, sock.txt
MD5	c5d712f82d5d37bb284acd4468ab3533, 34b3009590ec2d361f07cac320671410, d9c019182d88290e5489cdf3b607f982, 29e44e8994197bdb0c2be6fc5dfc15c2, c9e35b5c1dc8856da25965b385a26ec4, d1c5e7b8e937625891707f8b4b594314, ef6a213f59f3fbee2894bd6734bbaed2, ac58a214ce7deb3a578c10b97f93d9c3, c3b8f6d102393b4542e9f951c9435255, 0a5c4ad3ec240fbfd00bdc1d36bd54eb, ff52fdf84448277b1bc121f592f753c5, a2fd181f57548c215ac6891d000ec6b9, 625bd7275e1892eac50a22f8b4a6355d, db38ef2e3d4d8cb785df48f458b35090
Email Addresses	asauribe[@]tutanota[.]com, cringghost[@]skiff[.]com, crptbackup[@]skiff[.]com, d3crypt[@]onionmail[.]org, d3svc[@]tuta[.]io, eternalnightmare[@]tutanota[.]com, evilcorp[@]skiff[.]com, fileunlock[@]onionmail[.]org, fortihooks[@]protonmail[.]com, genesis1337[@]tutanota[.]com, ghost1998[@]tutamail[.]com, ghostbackup[@]skiff[.]com, ghosts1337[@]skiff[.]com, ghosts1337[@]tuta[.]io, ghostsbackup[@]skiff[.]com, hsharada[@]skiff[.]com, just4money[@]tutanota[.]com, kellyreiff[@]tutanota[.]com, kev1npt[@]tuta[.]io, lockhelp1998[@]skiff[.]com, r[.]heisler[@]skiff[.]com, rainbowforever[@]skiff[.]com, rainbowforever[@]tutanota[.]com, retryit1998[@]mailfence[.]com,

TYPE	VALUE
Email Addresses	retryit1998[@]tutamail[.]com, rsacrpthelp[@]skiff[.]com, rsahelp[@]protonmail[.]com, sdghost[@]onionmail[.]org, shadowghost[@]skiff[.]com, shadowghosts[@]tutanota[.]com, summerkiller[@]mailfence[.]com, summerkiller[@]tutanota[.]com, webroothooks[@]tutanota[.]com

Patch Links

https://www.fortiguard.com/psirt/FG-IR-18-384

https://helpx.adobe.com/coldfusion/kb/coldfusion-security-hot-fix-bulletin.html

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34473

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34523

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0604

References

https://www.cisa.gov/sites/default/files/2025-02/aa25-050a-stopransomware-ghost-cring-ransomware.pdf

https://www.broadcom.com/support/security-center/protection-bulletin/ghost-aka-cring-ransomware

https://hivepro.com/threat-advisory/unknown-iranian-attackers-leverage-vulnerabilities-to-conduct-ransom-operations/

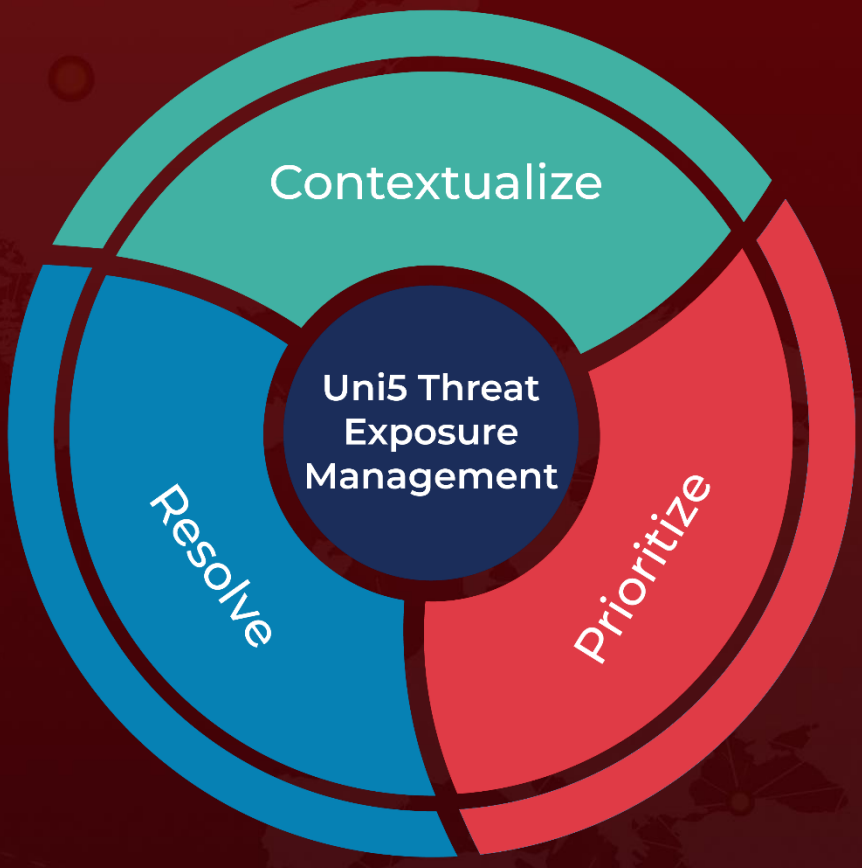
https://hivepro.com/threat-advisory/tropic-trooper-targets-middle-east-with-new-web-shell/

https://hivepro.com/threat-advisory/multiple-iranian-actors-have-launched-attacks-against-the-albanian-government/

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

February 25, 2025 • 3:00 AM

More at www.hivepro.com