Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

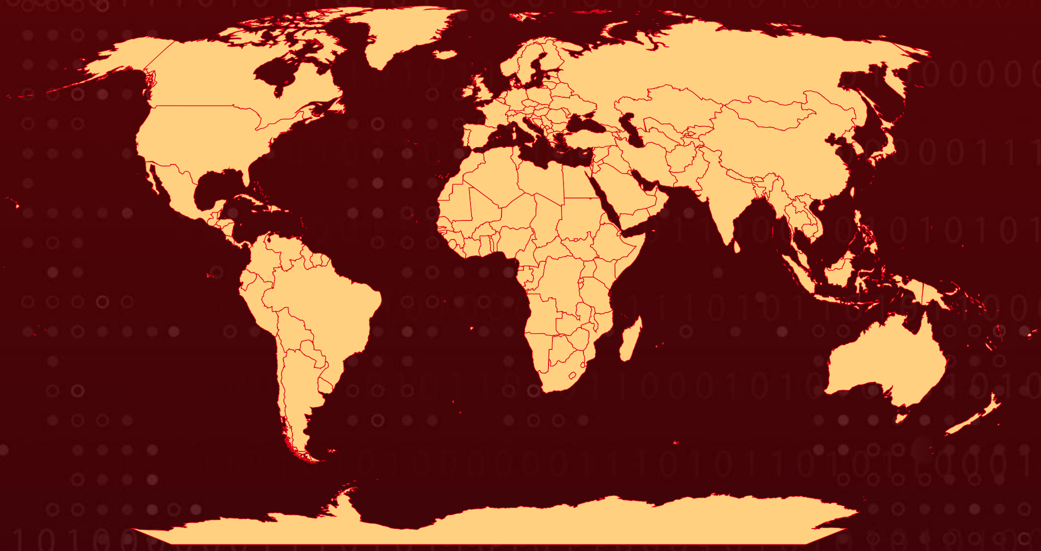
Fog Ransomware Variant Uses Intel Driver Flaw for Attack

Date of Publication	Admiralty Code	TA Number
April 15, 2025	A1	TA2025115

Summary

Active Since: 2025
Malware: DOGE BIG BALLS Ransomware
Targeted Region: Worldwide
Ransom: 4.721373 Monero (XMR) (~USD1000)
Attack: A newly discovered ransomware campaign, featuring a customized variant of the Fog ransomware rebranded as “DOGE BIG BALLS,” combines technical sophistication with psychological manipulation. Delivered through a finance-themed ZIP file, the attack leverages PowerShell scripting, a known Intel driver vulnerability, and precise geolocation to execute its payload. Beyond encryption, it draws attention for its bizarre ransom note.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2015-2291	Intel Ethernet Diagnostics Driver for Windows Denial-of-Service Vulnerability	iQVW32.SYS: before 1.3.1.0; iQVW64.SYS: before 1.3.1.0	✗	✓	✓

Attack Details

#1

A new ransomware campaign has surfaced featuring a modified version of the Fog ransomware, rebranded with the bizarre name "DOGE BIG BALLS." Beneath the campaign lies a technically sophisticated and psychologically manipulative operation, designed not just to encrypt files but to confuse, mislead, and intimidate.

#2

It begins with a finance-themed ZIP file titled "Pay Adjustment.zip," containing a disguised shortcut file. A single click silently triggers a PowerShell script that checks for administrative access, then downloads and executes multiple payloads. At its core, the attack exploits a known Intel driver vulnerability (CVE 2015 2291) using a Bring Your Own Vulnerable Driver tactic, granting kernel-level access to disable security features and escalate privileges.

#3

The payload masquerades as "Adobe Acrobat.exe," strategically installed depending on the user's permission level. It encrypts files with a ".flocked" extension, logs its actions, deletes shadow copies, and drops a ransom note. Victims are directed to a Tor site, asked for one thousand dollars in Monero, and in a strange twist, requested to list their top five work achievements.

#4

Beyond encryption, the malware collects detailed system data. It uses the Wigle API to geolocate victims through their router's MAC address, a method far more accurate than traditional IP-based tracking. A Havoc command and control beacon signals intentions that extend beyond ransom, suggesting long-term access or additional malicious activities.

#5

Adding a disturbing layer, the ransom note includes real personal details of a man and references Elon Musk's DOGE initiative. Bizarre statements accompany address, blending satire, misdirection, and defamation.

#6

Two scripts, stage1.ps1, and lootsubmit.ps1, handles persistence and system reconnaissance, while a tool named ktool.exe installs the vulnerable driver and performs low level operations with built in sandbox detection to avoid analysis. This campaign stands out not just for its technical expertise but for its calculated theatrics. It is targeted, layered, and deeply unsettling, blending precision hacking with unsettling psychological tactics.

Recommendations

Prioritize Patch Management for Known Exploits: Ensure timely patching of all known vulnerabilities, especially those exploited in the wild. In this case, CVE-2015-2291 is a critical flaw in an Intel driver that enabled kernel-level access. While the vulnerability is old, attackers continue to exploit it through BYOVD tactics so even legacy, or unused drivers must be reviewed and removed.

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.

Restrict Execution of Malicious File Types: Enforce Group Policy or AppLocker configurations to block the execution of .LNK files and untrusted or unsigned PowerShell scripts, which are frequently used as the initial infection vector in attacks like this.

Implement Behavioral Detection: Augment detection capabilities with behavior-based analytics. Focus on spotting rare persistence techniques and post-exploitation actions such as token stealing, driver tampering, and memory manipulation.

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	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	T1566 Phishing	T1566.001 Spearphishing Attachment
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1134 Access Token Manipulation	T1134.001 Token Impersonation/Theft	T1068 Exploitation for Privilege Escalation	T1027 Obfuscated Files or Information
T1218 System Binary Proxy Execution	T1218.005 Mshta	T1082 System Information Discovery	T1016 System Network Configuration Discovery
T1614 System Location Discovery	T1005 Data from Local System	T1105 Ingress Tool Transfer	T1486 Data Encrypted for Impact
T1490 Inhibit System Recovery	T1204 User Execution	T1204.002 Malicious File	T1036 Masquerading
T1036.004 Masquerade Task or Service	T1055 Process Injection	T1562 Impair Defenses	T1562.001 Disable or Modify Tools
T1041 Exfiltration Over C2 Channel	T1070.004 File Deletion	T1070 Indicator Removal	T1057 Process Discovery
T1070.009 Clear Persistence			

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//hilarious-trifle-d9182e[.]netlify[.]app/lootsubmit[.]ps1, hxxps[:]//hilarious-trifle-d9182e[.]netlify[.]app/cwiper[.]exe, hxxps[:]//hilarious-trifle-d9182e[.]netlify[.]app/ktool[.]exe, hxxps[:]//hilarious-trifle-d9182e[.]netlify[.]app/Pay%20Adjustment[.]zip, hxxps[:]//hilarious-trifle-d9182e[.]netlify[.]app/stage1[.]ps1
File Path	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\
SHA256	5402c5dc6656697b22a20e90f6ab7a2cd216ce7c70126ed0e855682035c299be, d802bdaad6713549b5098d3545e07794900869c01a68024a1282fea74d40c4a3, 4106345cd7a879597c5132b307f9c616e539616241d39a32393a1a8cd0c23452, ffe6f62b8e76fb8be1498e403941406a0f6a4dea8816878c27c031c78ca44045, ac6533a2702a16e90746ce9f84895e8d579314c0e18589610e4e281d5571a954, 44b7eebf7a26d466f9c7ad4ddb058503f7066aded180ab6d5162197c47780293, 3d2cbef9be0c48c61a18f0e1dc78501ddabfd7a7663b21c4fcc9c39d48708e91, f08b5316f6bc009d0cb41d4ce0086e615bf130b667cb2cdceecad07fda24fc49, 8e209e4f7f10ca6def27eabf31ecc0dbb809643feaecb8e52c2f194daa0511aa, 805b2f5cab2a4ba6088e6b6f91d6f1f0671c61092b571358969d69ff8c184c30, 30a6688899c22a3ce4c1b977fae762e3f7342d776e1aa2c90835e785d42f60c1, ecfed78315f942fe0e6762acd73ef7f30c34620615ef5e71f899e1d069dabd9e, 2c38a56beec1f7c8b919a1a2d9f9497358e763a1c8d9d71aa8a0e4ef062d3ec2, 4ad9216a0a6ac84a7b0b5593b0fc97e27de9cdfeb84ab7e5339ae5a4102100c0, 8d843c757aea85087a95794f93071bfacb7c4db06f33520308f39b97cf88cabb, 330e415ed1dd462486bd99676ef03bcc1da05c17ced655f82b2fbd0787e7dc8f, a59c40e7470b7003e8adfee37c77606663e78d7e3f2ebb8d60910af19924d8d

TYPE	VALUE
File Name	Pay Adjustment.zip, Adobe Acrobat.exe

Patch Link

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00051.html

References

https://cyble.com/blog/doge-big-balls-ransomware-edward-coristine/

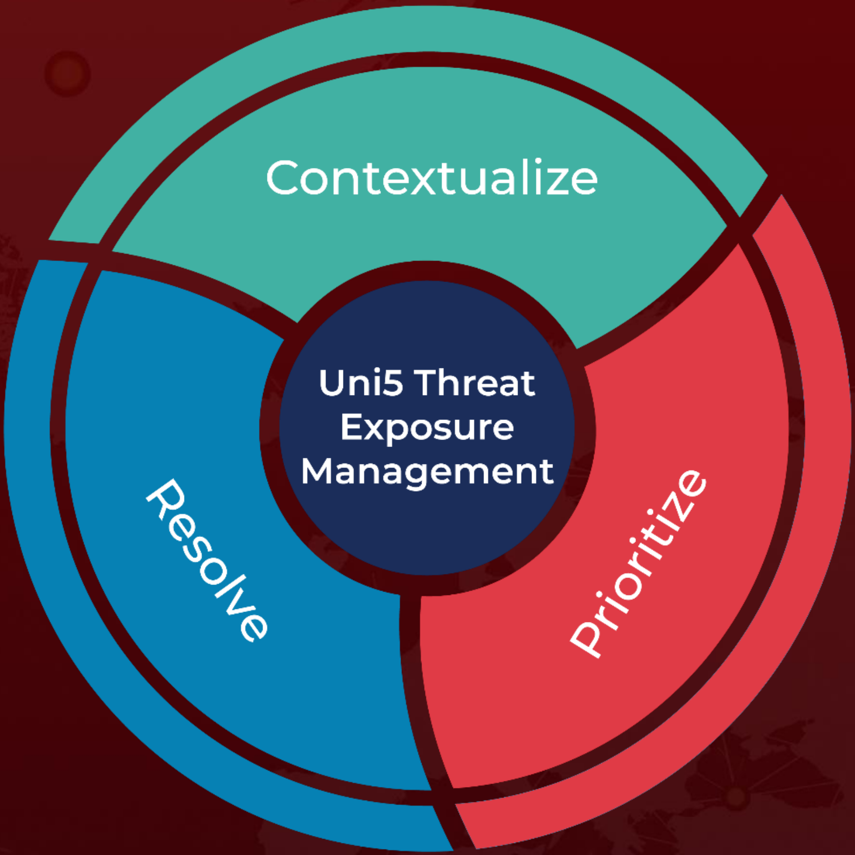
https://hivepro.com/threat-advisory/fog-ransomware-a-growing-threat-to-the-financial-industry/

https://hivepro.com/threat-digest/cisas-known-exploited-vulnerability-catalog-february-2023/

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

April 15, 2025 • 9:00 PM

More at www.hivepro.com