Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

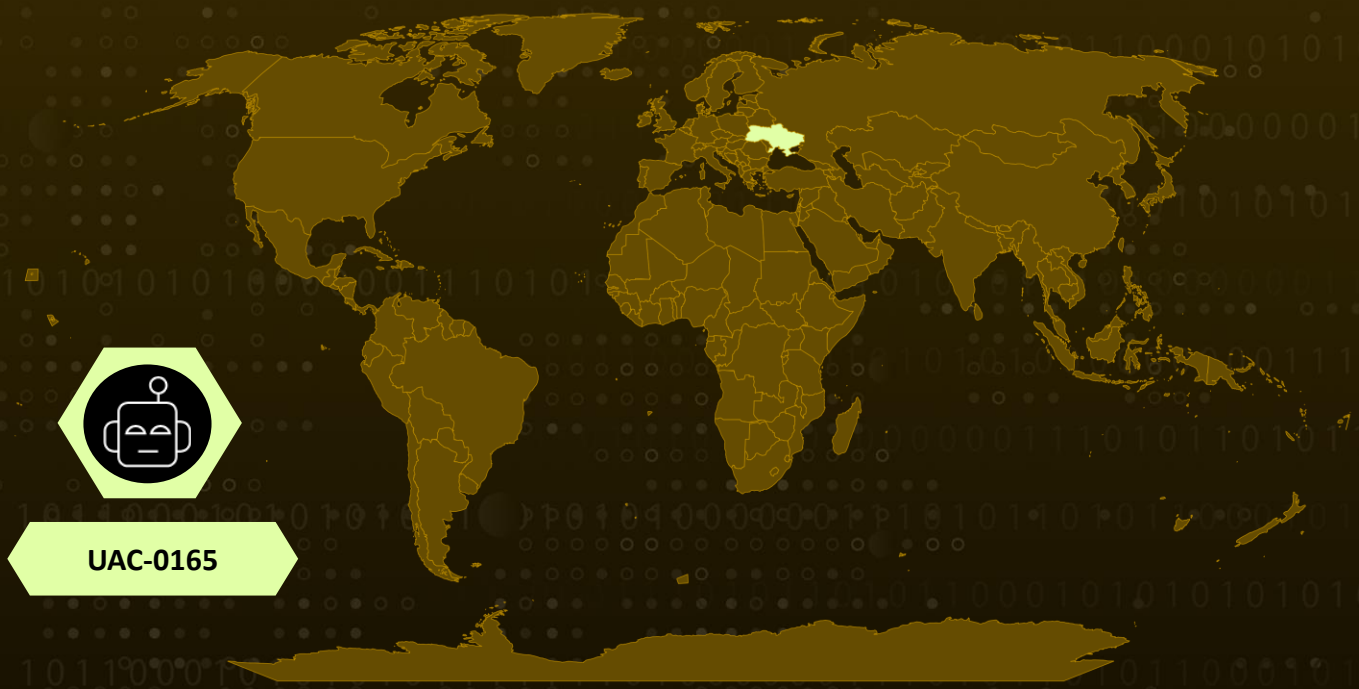
Unveiling AcidPour Evolution of Destructive Malware Targeting Ukraine

Date of Publication	Admiralty Code	TA Number
March 22, 2024	A1	TA2024114

Summary

Attack Began: March 16th, 2024
Targeted Countries: Ukraine
Malware: AcidPour, AcidRain
Affected Platform: Linux
Targeted Industries: Telecommunications, Critical Infrastructure, Energy, and Government
Threat Actor: UAC-0165
Attack: AcidPour, a variant of the destructive AcidRain wiper malware previously used during the Russia-Ukraine conflict, signals a heightened threat to Ukraine's critical infrastructure. By targeting Linux UBI and DM logic, AcidPour poses a significant risk to large storage devices and RAID arrays, potentially causing widespread disruptions. Urgent collaboration and monitoring efforts are essential to address this escalating cyber threat in Ukraine.

Attack Regions



Attack Details

#1

AcidPour, a newly discovered malware variant, has emerged as a serious threat to Ukraine's critical infrastructure. This destructive program, linked to the previously identified AcidRain wiper malware, targets embedded devices running Linux systems. AcidPour's capabilities extend beyond those of its predecessor, potentially allowing it to wipe not only individual devices but also RAID arrays and large storage units. This expanded destructive potential could cause widespread data loss and disrupt essential services in Ukraine.

#2

The discovery of AcidPour coincides with recent outages experienced by Ukrainian telecommunication networks. AcidPour employs similar wiping mechanisms to AcidRain, such as IOCTL-based wiping, indicating a shared lineage between the two. Notable additions in AcidPour include support for UBI and DM logic, enabling it to target a broader range of devices, including embedded systems. Additionally, AcidPour exhibits a self-delete function and an alternate device wiping mechanism, indicating a response to previous discoveries.

#3

Attribution of AcidPour activity is linked to UAC-0165, a subgroup of the Sandworm APT associated with Russian-linked threat activity in Ukraine. This potential connection raises serious concerns about Russian involvement in the current cyberattacks targeting Ukraine.

#4

The devastating impact of wiper malware is no stranger to Ukraine. In February 2022, AcidRain attacks rendered Eutelsat KA-SAT modems inoperable, causing disruptions across Europe. The deployment of AcidPour against Ukrainian infrastructure in 2024 suggests a potential repeat of such large-scale damage.

#5

The discovery of AcidPour highlights the evolving nature of cyber threats in the ongoing conflict, with threat actors demonstrating enhanced technical capabilities and strategic targeting of critical infrastructure. Continued monitoring and collaboration within the research community are crucial to understanding and mitigating these evolving threats.

Recommendations

Update Security Measures: Ensure that all security measures, including antivirus, firewalls, and intrusion detection systems, are up to date. Regularly update security patches and definitions to detect and block known threats, including variants of AcidPour.

Incident Response Planning: Develop and regularly update incident response plans specifically tailored to address wiper malware attacks like AcidPour. This should include procedures for detecting, containing, and recovering from such incidents.

Monitoring and Detection: Deploy advanced threat detection and monitoring tools capable of identifying and mitigating wiper malware attacks in real-time. This includes behavior-based analytics, intrusion detection systems, and endpoint protection solutions.

Behavior-Based Detection: Employ behavior-based detection techniques to identify and block unusual or suspicious activity on endpoints and network devices. Monitor for signs of unauthorized access, data exfiltration, or abnormal system behavior that may indicate the presence of AcidPour or similar threats.

Potential MITRE ATT&CK TTPs

TA0040 Impact	TA0005 Defense Evasion	T1486 Data Encrypted for Impact	T1529 System Shutdown/Reboot
T1495 Firmware Corruption	T1070.004 File Deletion	T1070 Indicator Removal	T1498 Network Denial of Service
T1489 Service Stop	T1561 Disk Wipe		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	1bde1e4ecc8a85cffef1cd4e5379aa44
SHA1	b5de486086eb2579097c141199d13b0838e7b631
IPv4	185[.]61[.]137[.]155
SHA256	6a8824048417abe156a16455b8e29170f8347312894fde2aabe644c4995d7728
Domains	solntsepek[.]com, solntsepek[.]info, solntsepek[.]org, solntsepek[.]ru

References

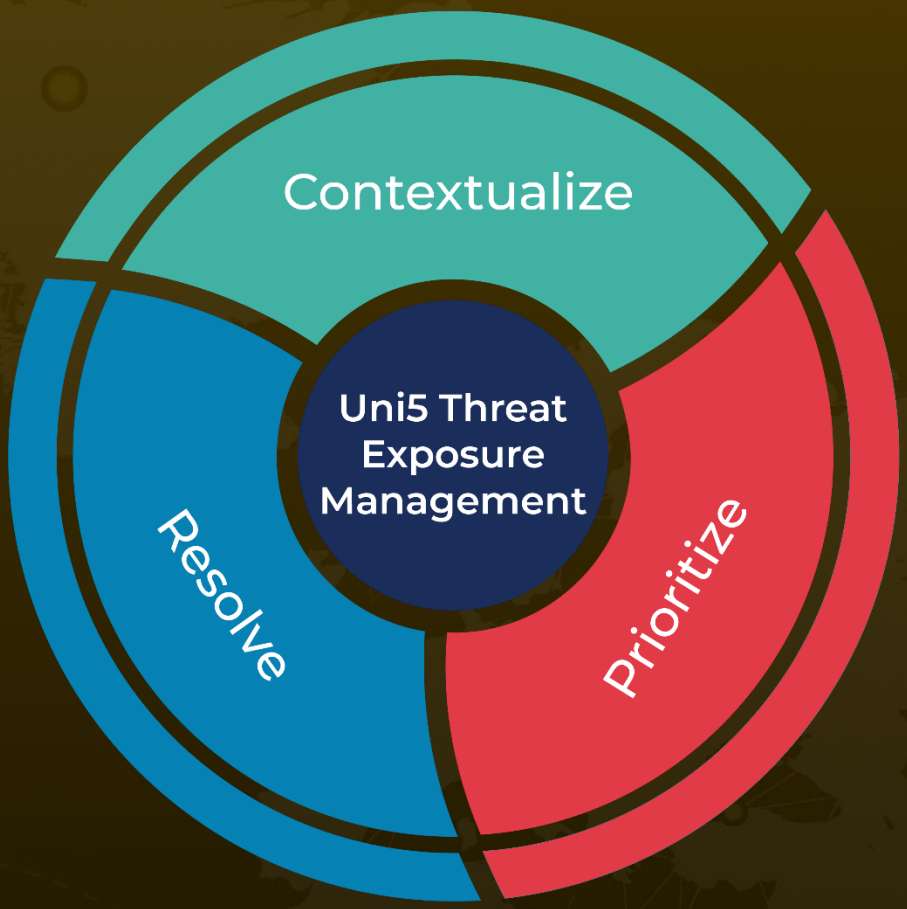
https://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/

https://www.hivepro.com/threat-advisory/cyber-attack-on-ukrainian-national-information-agency/

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

March 22, 2024 • 4:30 AM

More at www.hivepro.com