Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

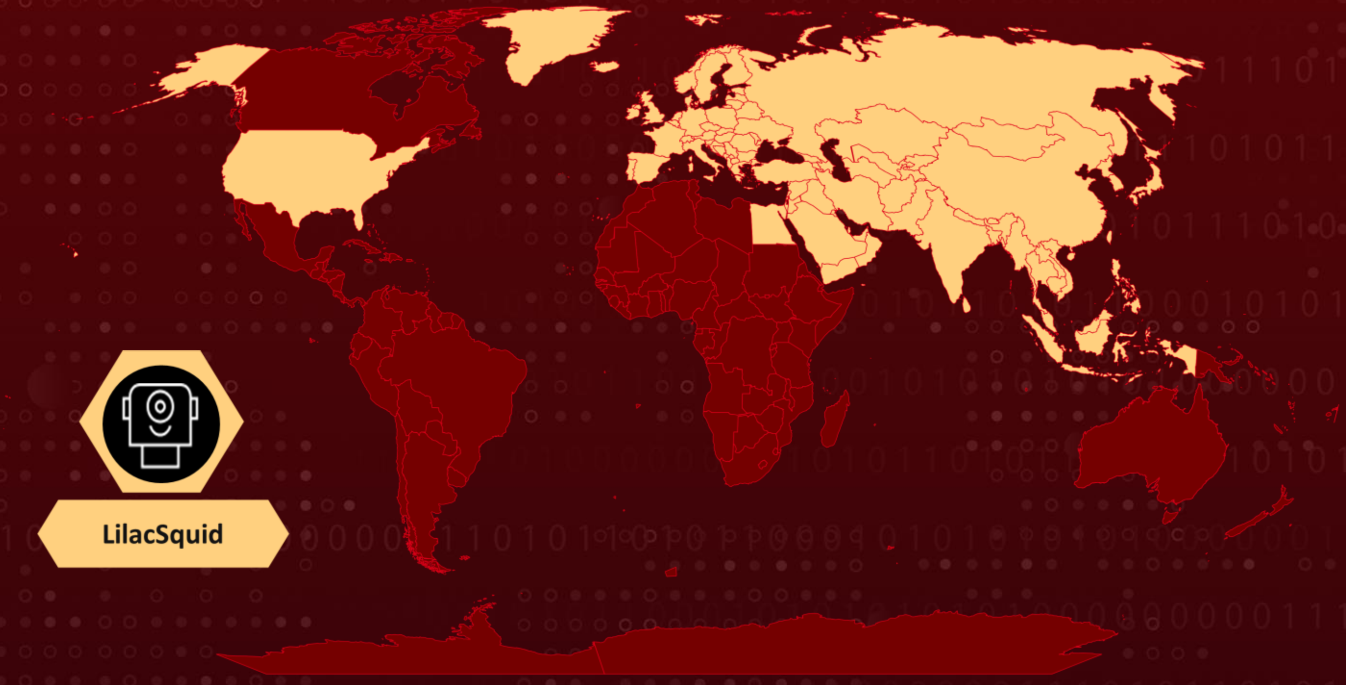
Deciphering LilacSquid's Strategies for Long-Term Data Theft

Date of Publication	Admiralty code	TA Number
June 6, 2024	A1	TA2024216

Summary

Active Since: 2021
Threat Actor: LilacSquid (aka UAT-4820)
Malware: MeshAgent, PurpleInk, InkBox, InkLoader
Targeted Industries: Information Technology, Research, Industrial, Energy, Pharmaceutical, Oil and Gas
Targeted Regions: United States, Europe, Asia

Actor Map



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

Actor Details

#1

An emerging data theft campaign, orchestrated by a newly identified threat actor, utilizes tools similar to those used by North Korean APT groups. This group, known as LilacSquid, has been active since at least 2021. The campaign deploys MeshAgent and a customized version of QuasarRAT, termed PurpleInk, as primary implants after successfully breaching vulnerable internet-exposed application servers.

#2

LilacSquid specifically targets IT organizations in the United States, energy sectors across Europe, and pharmaceutical companies in Asia. Some of their tactics overlap with those of **Andariel**, a North Korean threat actor that operates as a sub-group within the notorious Lazarus Group.

#3

LilacSquid's main objective is to establish prolonged access to compromised entities to exfiltrate valuable data to servers under the attackers' control. To gain initial access, LilacSquid employs various techniques, including exploiting vulnerabilities in public-facing application servers and using compromised RDP credentials.

#4

Inside the attack chain, LilacSquid utilizes multiple open-source tools such as MeshAgent, a remote management tool, to establish connections with attacker-controlled command-and-control servers and conduct reconnaissance. Additionally, they use InkLoader, a .NET-based loader, to read from a predefined file path on the disk and decrypt its contents.

#5

MeshAgent and InkLoader facilitate the deployment of custom malware such as PurpleInk, a sophisticated version of the QuasarRAT Trojan. PurpleInk is extensively obfuscated and highly versatile. It can execute new applications, perform file operations, gather system information, enumerate directories and running processes, launch a remote shell, and connect to a specific remote address designated by a command-and-control server. The LilacSquid campaign underscores the persistent and evolving threat posed by sophisticated APT actors through their strategic use of both open-source tools and custom malware.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
LilacSquid (aka UAT-4820)	-	United States, Europe, Asia	Information Technology, Research, Industrial, Energy, Pharmaceutical, Oil and Gas
	MOTIVE		
	Information Theft, Espionage		

Recommendations

Regular Vulnerability Assessments: Conduct frequent vulnerability assessments on public-facing application servers to identify and patch potential weaknesses that could be exploited by threat actors like LilacSquid.

Enhance Network Monitoring: Invest in robust network monitoring and intrusion detection systems to quickly detect and respond to suspicious activities. Early detection can mitigate the damage caused by potential breaches.

Harden Server Configurations: Apply server hardening techniques to reduce the attack surface by disabling unnecessary services, closing unused ports, and following industry best practices for server security.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery

TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration	T1584 Compromise Infrastructure
T1584.004 Server	T1587 Develop Capabilities	T1587.001 Malware	T1190 Exploit Public-Facing Application
T1059 Command and Scripting Interpreter	T1543 Create or Modify System Process	T1055 Process Injection	T1005 Data from Local System
T1001 Data Obfuscation	T1573 Encrypted Channel	T1105 Ingress Tool Transfer	T1041 Exfiltration Over C2 Channel

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	2eb9c6722139e821c2fe8314b356880be70f3d19d8d2ba530adc9f466ffc67d8
IPv4	67[.]213[.]221[.]6, 192[.]145[.]127[.]190, 45[.]9[.]251[.]14, 199[.]229[.]250[.]142

References

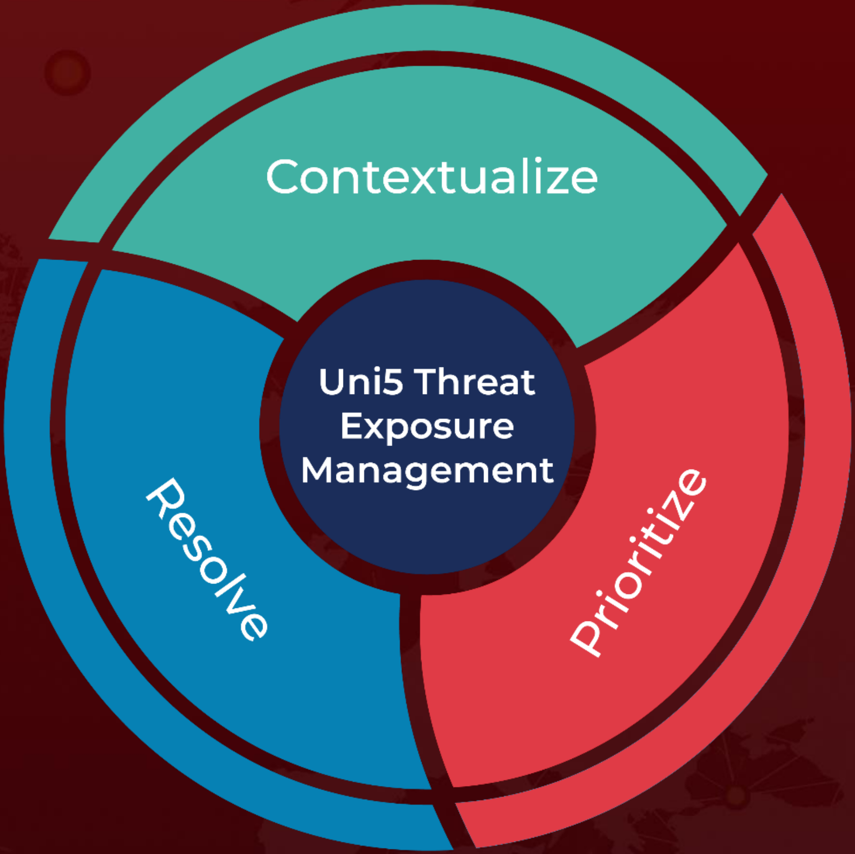
https://blog.talosintelligence.com/lilacsquid/

https://www.hivepro.com/threat-advisory/andariel-group-unleashes-new-earlyrat-malware/

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

June 6, 2024 • 5:30 AM

More at www.hivepro.com