Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

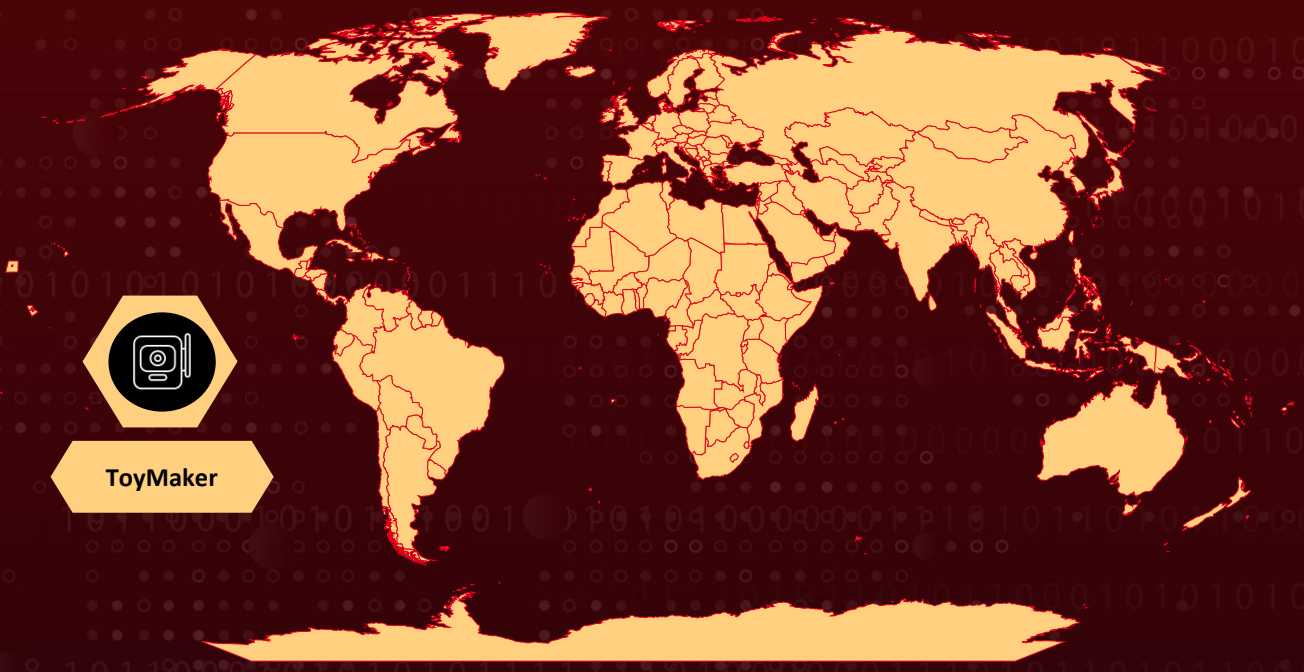
ToyMaker: Unveiling the Role of Initial Access Brokers in Ransomware Attacks

Date of Publication	Admiralty Code	TA Number
April 25, 2025	A1	TA2025129

Summary

Attack Commenced: 2023
Targeted Region: Worldwide
Targeted Platform: Windows
Threat Actor: ToyMaker
Malware: LAGTOY, Cactus ransomware
Targeted Industry: Critical infrastructure
Attack: In 2023, ToyMaker, an Initial Access Broker, breached a critical infrastructure network using a custom backdoor called LAGTOY. The actor harvested credentials and established persistence before handing off access to the Cactus ransomware group. Weeks later, Cactus conducted reconnaissance, deployed remote tools, and executed a ransomware attack. The operation shows coordinated collaboration between initial access brokers and ransomware operators.

Attack Regions



Attack Details

#1

A sophisticated cyberattack campaign in 2023 involved an Initial Access Broker (IAB) known as ToyMaker, who collaborates with ransomware groups, notably the Cactus gang. In this significant breach of a critical infrastructure organization, ToyMaker was identified as the actor responsible for the initial compromise. The breach was executed by exploiting internet-facing vulnerabilities and deploying a custom backdoor tool named “LAGTOY.” This implant enabled ToyMaker to gain persistent access to the network through reverse shell connections and remote command execution.

#2

Following the initial infiltration, ToyMaker focused on credential extraction and lateral movement within the environment. The actor used forensic memory analysis tools, including Magnet RAM Capture, to harvest credentials, which were then used to create and maintain fake user accounts. These steps helped solidify ToyMaker’s foothold in the network while setting the stage for the subsequent ransomware phase. After conducting these preparatory actions, ToyMaker ceased activity, suggesting a clear role as the access enabler.

#3

Several weeks later, the Cactus ransomware gang leveraged the access previously established by ToyMaker. Cactus initiated comprehensive network reconnaissance and deployed a variety of remote management tools, including eHorus, RMS, and AnyDesk, to maintain access. They eventually executed the ransomware payload, exfiltrated sensitive data, and deleted shadow volume copies to prevent data recovery. The progression of this attack illustrates a well-planned and methodical handoff between ToyMaker and Cactus, indicative of organized collaboration.

Recommendations

Patch Internet-Facing Systems Promptly: Regularly identify and patch vulnerabilities in internet-facing services, applications, and operating systems. Prioritize updates for critical infrastructure components and use vulnerability scanning tools to assess exposure.

Implement Network Segmentation: Isolate critical systems from user-accessible environments and limit lateral movement through strict access controls and internal firewalls. Enforce the principle of least privilege for user and service accounts.

Deploy Endpoint Detection and Response (EDR) Tools: Use advanced EDR solutions to detect and respond to suspicious behaviors, including credential dumping tools and custom backdoors like LAGTOY. Monitor for unusual PowerShell or command-line activity.

Monitor and Restrict Remote Access Tools: Audit and restrict the use of remote access tools such as AnyDesk, RMS, and eHorus. Implement application allowlisting and alert on unauthorized installations of remote administration software.

Harden Credential Security: Enforce strong authentication mechanisms, including multi-factor authentication (MFA), especially for remote access and privileged accounts. Regularly rotate passwords and monitor for signs of credential misuse.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0040 Impact	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
T1190 Exploit Public-Facing Application	T1562.001 Disable or Modify Tools	T1562 Impair Defenses	T1082 System Information Discovery
T1590 Gather Victim Network Information	T1136 Create Account	T1003 OS Credential Dumping	T1560 Archive Collected Data
T1048 Exfiltration Over Alternative Protocol	T1543 Create or Modify System Process	T1018 Remote System Discovery	T1070 Indicator Removal
T1070.007 Clear Network Connection History and Configurations	T1070.009 Clear Persistence	T1608.001 Upload Malware	T1070.003 Clear Command History

T1608 Stage Capabilities	T1218.007 Msiexec	T1218 System Binary Proxy Execution	T1053 Scheduled Task/Job
T1053.005 Scheduled Task	T1021.004 SSH	T1021 Remote Services	T1222 File and Directory Permissions Modification
T1222.001 Windows File and Directory Permissions Modification	T1059.003 Windows Command Shell	T1098 Account Manipulation	T1490 Inhibit System Recovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	fdf977f0c20e7f42dd620db42d20c561208f85684d3c9efd12499a3549be3826, 0a367cc7e7e297248fad57e27f83316b7606788db9468f59031fed811cfe4867, 0bcfea4983cfc2a55a8ac339384ecd0988a470af444ea8f3b597d5fe5f6067fb, 5831b09c93f305e7d0a49d4936478fac3890b97e065141f82cda9a0d75b1066d, 691cc4a12fbada29d093e57bd02ca372bc10968b706c95370daeee43054f06e3, 70077fde6c5fc5e4d607c75ff5312cc2fdf61ea08cae75f162d30fa7475880de, a95930ff02a0d13e4dbe603a33175dc73c0286cd53ae4a141baf99ae664f4132, c1bd624e83382668939535d47082c0a6de1981ef2194bb4272b62ecc7be1ff6b
IPv4	209[.]141[.]43[.]37, 194[.]156[.]98[.]155, 158[.]247[.]211[.]51, 39[.]106[.]141[.]68, 47[.]117[.]165[.]166, 195[.]123[.]240[.]2, 75[.]127[.]0[.]235, 149[.]102[.]243[.]100,

TYPE	VALUE
IPv4	206[.]188[.]196[.]20, 51[.]81[.]42[.]234, 178[.]175[.]134[.]52, 162[.]33[.]177[.]56, 64[.]52[.]80[.]252, 162[.]33[.]178[.]196, 103[.]199[.]16[.]92

References

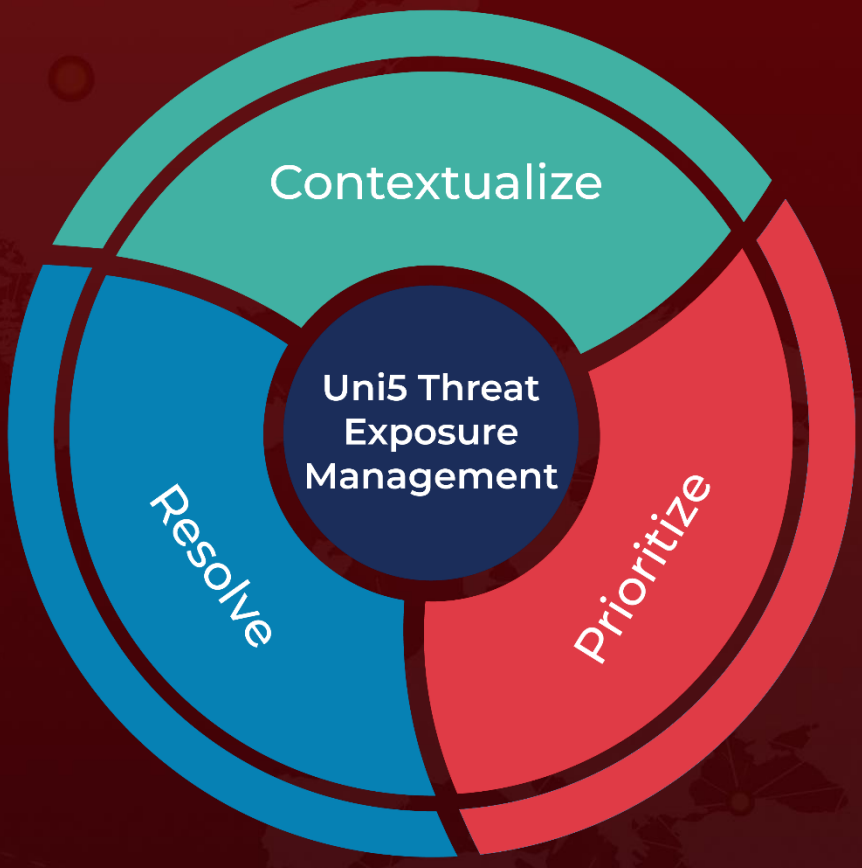
https://blog.talosintelligence.com/introducing-toymaker-an-initial-access-broker/

https://www.hivepro.com/cactus-ransomware-emerges-as-new-threat-targeting-large-enterprises/

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 25, 2025 • 7:00 AM

More at www.hivepro.com