SEQURETEK
SIMPLIFY SECURITY

Cyber Threat Advisory - SQTK/ADV/2024/0042

DarkGate Malware Delivered Through Phishing Emails with "Paste-and-Run" Attack (IoCs)

Indicators of Compromise

Hashes

IOC	Type of File /File names
8b788345fe1a3e9070e2d2982c1f1eb2	HTML
a66cc0139c199b37a32731592fb3ac0b	header.png
0b77babfa83bdb4443bb3c5f918545ae	qhsddxna
404bd47f17d482e139e64d0106b8888d	script.a3x (in xcdttafq)
4b653886093a209c3d86cb43d507a53f	HTML
30e2442555a4224bf15bbffae5e184ee	dark.hta
7484931957633b796f165061b0c59794	rdyjyany
e0173741b91cabfecd703c20241c1108	script.a3x (in yoomzhda)
318f00b609039588ce5ace3bf1f8d05f	HTML
a77beccca5571c00ebc9e516fd96ce8	1.hta
f2e4351aa516a1f2e59ade5d9e7aa1d6	umkglnks
4d52ea9aa7cd3a0e820a9421d936073f	script.a3x (in iinkqrwu)

Download URLs

Download URLs
hxxps://jenniferwelsh[.]com/header.png
hxxp://mylittlecabbage[.]net/qhsddxna
hxxp://mylittlecabbage[.]net/xcdttafq
hxxps://linktoxic34[.]com/wp-content/themes/twentytwentytwo/dark.hta
hxxp://dogmupdate[.]com/rdyjyany
hxxp://dogmupdate[.]com/yoomzhda
hxxps://www.rockcreekdds[.]com/wp-content/1.hta
hxxp://flexiblemaria[.]com/umkglnks
hxxp://flexiblemaria[.]com/iinkqrwu

MITRE ATT&CK TACTICS AND TECHNIQUES

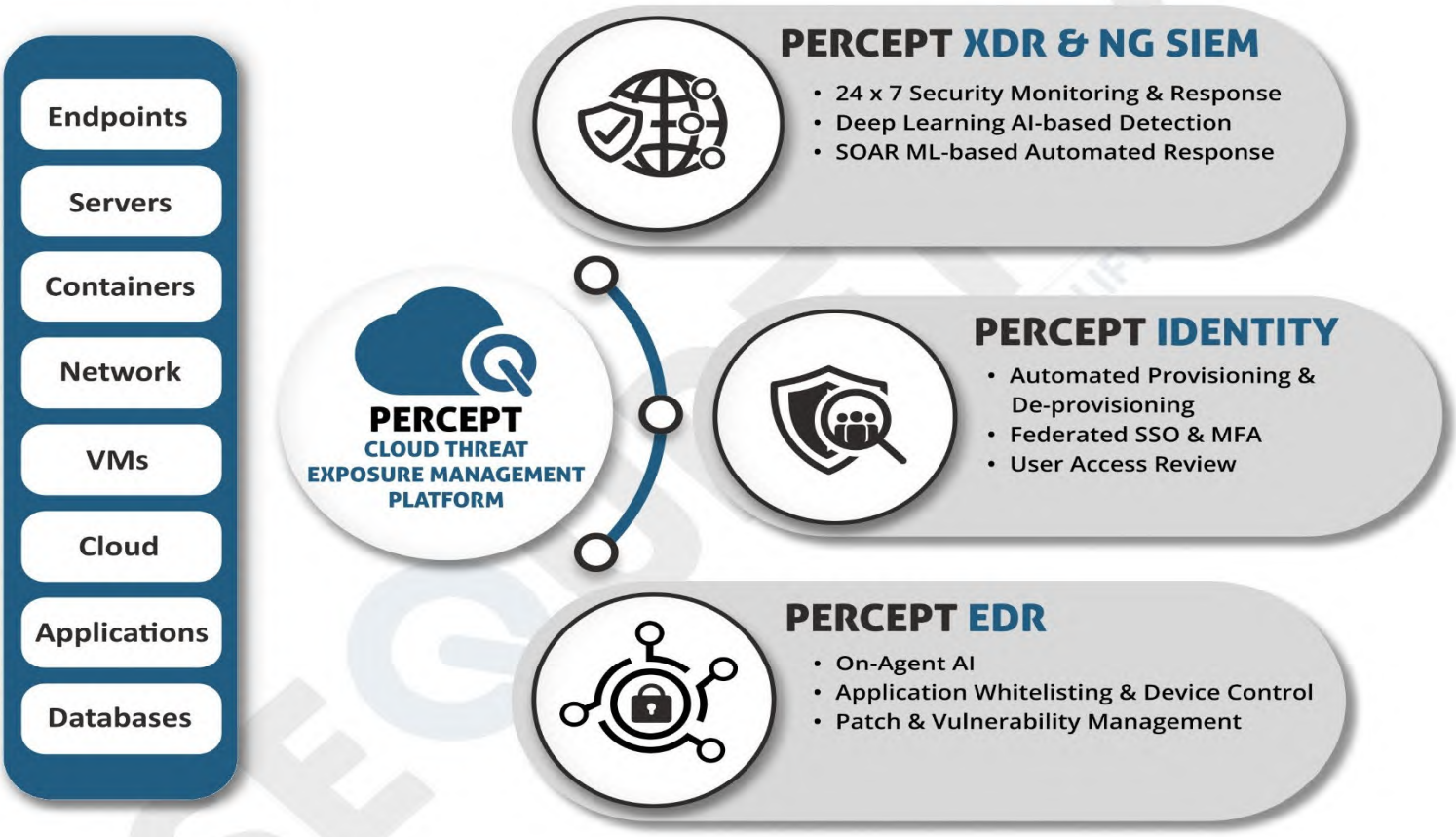
Technique Title	ID	Use
Initial Access		
Phishing: Spearphishing Attachment	T1566.001	Attackers initiate phishing campaign with malicious HTML attachments.
Execution		
User Execution	T1204	Users are tricked into executing malicious code by clicking on "How to Fix" button.
Command and Scripting Interpreter: PowerShell	T1059.001	Malicious JavaScript encodes PowerShell commands to be executed by the user.
Persistence		
Boot or Logon Autostart Execution	T1547.001	PowerShell script establishes persistence by downloading and executing HTA files.
Defense Evasion		
Obfuscated Files or Information	T1027	DarkGate malware and AutoIt scripts are obfuscated to evade detection.
Collection		
Clipboard Data	T1115	JavaScript saves decoded PowerShell command to clipboard for execution.
Input Capture	T1056.001	HTA file captures input to execute PowerShell commands from C2 server.
Command and Control		
Data Encoding	T1132	Base64 encoding is used to hide malicious PowerShell commands.
Commonly Used Port	T1043.001	DarkGate malware uses standard ports to communicate with C2 servers.
Exfiltration		
Data from Local System	T1030	DarkGate malware exfiltrates data from infected systems.
Impact		
System Shutdown/Reboot	T1529.002	DarkGate malware may initiate system shutdowns as part of its impact.
Account Access Removal	T1531	DarkGate malware may disable or remove user accounts on the compromised system.
Data Encrypted for Impact	T1486	DarkGate malware might encrypt data on the infected system to cause impact

10 YEARS | SEQURETEK
SIMPLIFY SECURITY

Trusted by Global Customers, Investors, and Partners

About Sequretek

Sequretek is a global cybersecurity company that offers end-to-end security in the areas of enterprise threat monitoring, incident response, device security, identity & access governance through our own AI powered Percept Cloud Threat Exposure Management Platform.



Take Control of Your Enterprise Security

- Enterprise scale, easy to use, and cloud native
- AI-driven threat detection, protection, remediation, and response
- Quick implementation and integration capabilities
- End-to-End ownership and management of Sequretek products
- Reduced Total Cost of Ownership (TCO) while simplifying security
- Out-of-the-box reporting for compliance and audit purposes

Feel free to reach out to us at info@sequretek[.]com to know more about our products, or schedule a demo at https[:]//sequretek[.]com/request-a-demo/

©SEQURETEK