K logix
Be confident.

NOVEMBER 2024 | THREAT INTEL NEWSLETTER

Hiring Hazard: More_eggs and COVERTCATCH

C-Suite level threat review by applicable business area addressing active threats.

In today's competitive job market, organizations rely on effective talent acquisition strategies such as social media recruitment and skill assessments to attract top talent. However, sophisticated malware campaigns like More_eggs and COVERTCATCH present threats to these recruitment processes. More_eggs has recently been used in a campaign targeting recruiters and executives while COVERTCATCH has been utilized targeting jobseekers. Both malware campaigns not only disrupt recruitment efforts, but also seek to compromise sensitive information.

More_eggs Malware:

More_eggs is a Malware-as-a-Service (MaaS) linked to the threat actor known as Golden Chickens, also referred to as Venom Spider. Since the malware's emergence in 2017, it has been used in campaigns targeting the financial and recruitment sector. Various threat actors, such as FIN6 and the Cobalt group, have utilized this MaaS to steal credentials from online bank accounts and IT administration accounts. Most recently, More_eggs has been distributed by a threat actor, believed by some analysts to be FIN6, to deceive recruiters into engaging with fake, malicious job applications.

COVERTCATCH Malware:

COVERTCATCH is a malware campaign attributed to Noth Korean threat actors that grew in prominence in 2024. This malware is used to target code-developers and finance employees looking for jobs. Through deceptive LinkedIn recruitment tactics, threat actors utilize fake job offers and social engineering to deliver the malware disguised as coding challenges. In recent attacks, malware disrupts talent acquisition efforts and compromises victims' systems to seek information such as cryptocurrency wallet keys. If employees engage in these coding challenges with their company computers, organizations could face significant risks.

More_eggs

Threat Level: Medium

Attack:

More_eggs is a sophisticated backdoor malware commonly delivered through spear-phishing emails targeting individuals (MITRE T1566.002). In a recent campaign utilizing this malware, phishing emails entice recruiters to download malicious ZIP files disguised as resumes (MITRE T1204.002). Upon execution, the malware conducts host reconnaissance to check if the environment is being run with administrator or user privileges, which influences its subsequent actions (MITRE T1592). If it detects administrator access, it may employ more extensive payloads to maximize its impact. The malware establishes persistence by modifying registry settings to have the malware automatically execute its functions when a user starts a new session (MITRE T1547.001). More_eggs then connects to a command-and control (C2) server to receive further malicious payloads, including infostealers and ransomware.

Remediation:

- Educate employees to use caution when opening attachments from unknown senders.
- Identify an EDR solution that best fits your environment.
- Educate employees on common threat vectors they may encounter in their respective jobs.

COVERTCATCH

Threat Level: Low

Attack:

COVERTCATCH is designed to target jobseekers with deceptive LinkedIn recruitment schemes (MITRE T1566.002). After engaging in a short conversation to build trust, attackers deploy fake job offers and social engineering tactics, to lure victims into downloading malware disguised as coding challenges (MITRE T1204.002). These ZIP files, which appear legitimate, execute a dropper that installs a second-stage payload, compromising macOS systems. This malware establishes persistence through mechanisms with background processes, such as Launch Agents and Daemons, ensuring ongoing access to the compromised environment even if the system is shut off (MITRE T1547.001). Furthermore, COVERTCATCH connects to a C2 server, allowing attackers to orchestrate further malicious actions such as keylogging and exfiltrating sensitive data (MITRE T1071).

Remediation:

- Consider prohibiting activities on company computers that are outside a user's job scope, such as conducting job interviews or skill assessments for an external organization.
- Set up monitoring for unusual network activity, especially connections to unknown servers.
- Implement whitelisting to ensure only approved applications can run on your organization's systems.

More_eggs:

- **More_eggs Tactics:** https://www.trendmicro.com/en_us/research/24/i/mdr-in-action--preventing-the-moreeggs-backdoor-from-hatching--.html
- **More_eggs Attack Information:** https://thehackernews.com/2024/06/moreeggs-malware-disguised-as-resumes.html

COVERTCATCH:

- **Deployment of COVERTCATCH:** https://thehackernews.com/2024/09/north-korean-threat-actors-deploy.html
- **COVERTCATCH Key Details:** https://cybersecsentinel.com/fake-linkedin-job-offers-hide-dangerous-malware/

How K logix Can Help

Technology Advisory

- Email Security
- Endpoint Detection and Response (EDR)
- Identity and Access Management (IAM)
- Managed Security Service Provider (MSSP)
- Security Information and Event Management (SIEM)
- Cloud Security Posture Management (CSPM)
- SaaS Security Posture Management (SaaS)

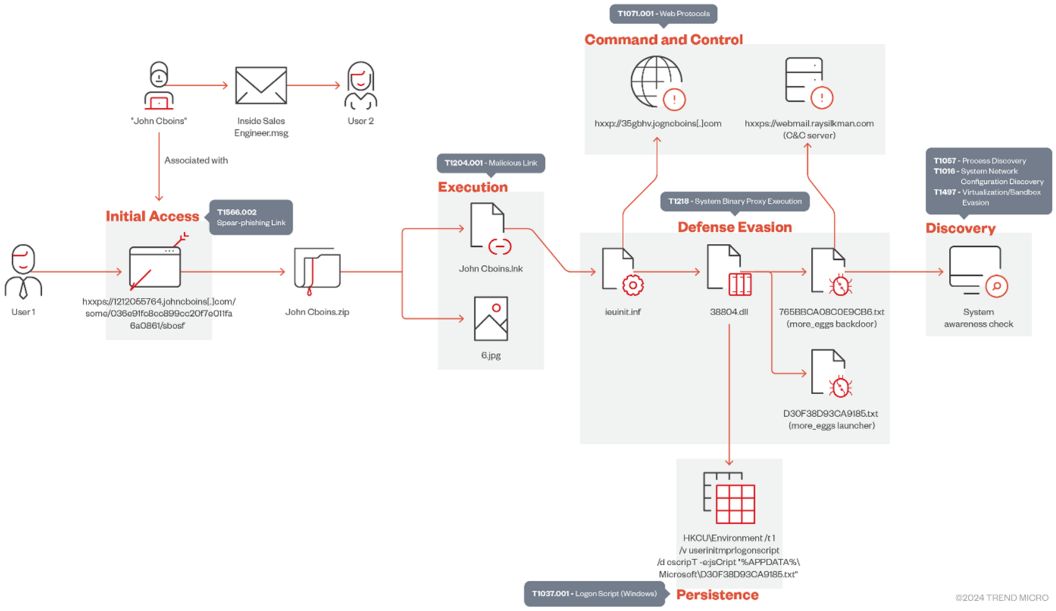
Program Advisory

- Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
- Cloud Security Maturity
- Identity and Access Management Program Maturity

Threat Intelligence

- Notification to customers of threats
- On-demand briefings
- Threat exposure workshops
- User awareness training seminars
- Monthly and quarterly threat intelligence reports

More_eggs Infection Diagram


"John Cboins"
Inside Sales Engineer.msg
User 2
Associated with
Initial Access
T1566.002 Spear-phishing Link
User 1
hxxps://1212055764.johncboins[.]com/some/036e91fc8cc899cc20f7e011fa6a0861/sbosf
John Cboins.zip
T1204.001 - Malicious Link
Execution
John Cboins.lnk
6.jpg
T1071.001 - Web Protocols
Command and Control
hxxp://35gbhv.jogncboins[.]com
hxxps://webmail.raysilkman.com (C&C server)
T1218 - System Binary Proxy Execution
Defense Evasion
ieuinit.inf
38804.dll
765BBCA08C0E9CB6.txt (more_eggs backdoor)
D30F38D93CA9185.txt (more_eggs launcher)
T1057 - Process Discovery
T1016 - System Network Configuration Discovery
T1497 - Virtualization/Sandbox Evasion
Discovery
System awareness check
HKCU\Environment /t 1 /v userinitmprlogonscript /d cscripT -e:jsCript "%APPDATA%\Microsoft\D30F38D93CA9185.txt"
T1037.001 - Logon Script (Windows)
Persistence
©2024 TREND MICRO

Source: https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/i/mdr-in-action--preventing-the-more_eggs-backdoor-from-hatching/MDR_More_eggs_Backdoor-Fig1-2.png

ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.