K logix

BE CONFIDENT.

VOL 3 | DECEMBER 2022 | THREAT INTEL NEWSLETTER

Mustang Panda and Lazarus Group

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

Nation-state threat actors are active at this time, including the Chinese Mustang Panda and North Korean Lazarus Group. Mustang Panda targets the research community attempting to gather scientific data and is also known to target diplomats. Lazarus Group is known for cybercrime in the banking industry and appears to be utilizing an updated backdoor to download, delete, and exfiltrate data in manufacturing and research. Both threat actors seem to have similar targets.

Mustang Panda

A cyber espionage group targeting google drive accounts in the research community is using phishing attacks to install custom malware. The phishing link targets Google Drive or Dropbox, making it look like an expected behavior after opening an email. The threat group Mustang Panda has been active in the past few months, attempting to gather scientific and diplomatic information.

Lazarus Group

North Korean crime-based threat actor appears to be targeting manufacturing and research with an update to the backdoor Dtrack. Dtrack was known for a nuclear power attack in India. The actor seems to have modified the tool to better hide in valid programs using three layers of encryption and obfuscation to avoid detection and analysis of capabilities.

Mustang Panda

Threat Level: Medium

Attack:

The threat group uses two new malware capabilities and one known strain called PubLoad. PubLoad creates persistence in the environment by adding registry keys and scheduling activities for Command and Control (C2) communications. The backdoor, ToneShell, is loaded into memory and hides after being installed by ToneIns.

Remediation:

- Monitor executed commands and arguments that may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key.
- Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations.

Lazarus Group

Threat Level: Medium

Attack:

Lazarus Group updated Dtrack backdoor used in the past against a nuclear power plant in India and most recently as part of Maui ransomware attacks. The new updates include concealing measures to avoid detection and analysis with a legitimate program and encryption. The payload is injected into the Windows File Explorer process with a keylogger and tools for screenshots.

Remediation:

- Monitor for changes made to files for unexpected modifications that attempt to hide artifacts.
- Monitor for newly executed processes that attempt to hide artifacts of an intrusion, such as common archive file applications and extensions (ex: Zip and RAR archive tools), and correlate with other suspicious behavior to reduce false positives from normal user and administrator behavior.

K logix

BE CONFIDENT.

VOL 3 | DECEMBER 2022 | THREAT INTEL NEWSLETTER

Mustang Panda Details

- **Pubload research:** https://blog.talosintelligence.com/mustang-panda-targets-europe/
- **Mustang Panda threat group information:** https://attack.mitre.org/groups/G0129/

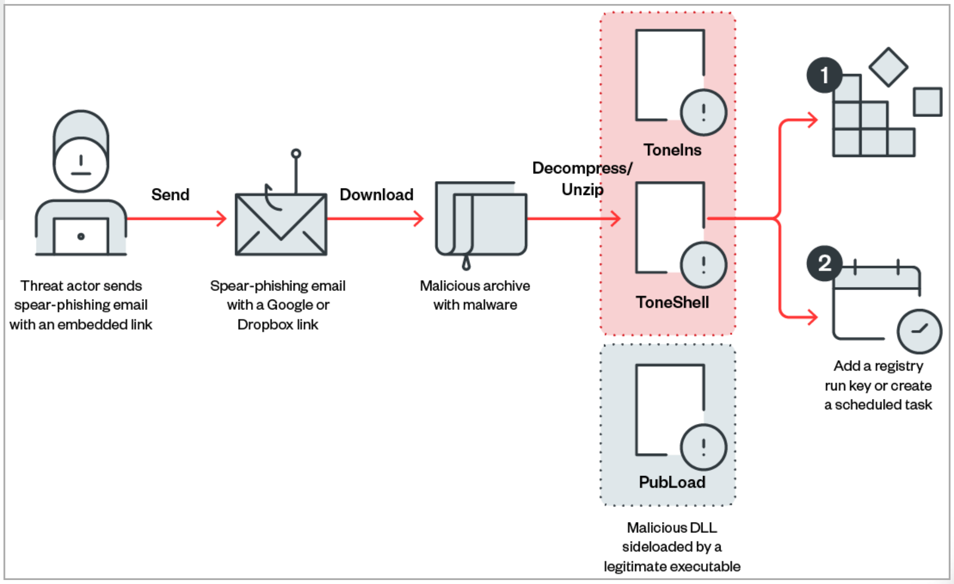
Lazarus Group Details

- **DTrack details from MITRE ATT&CK:** https://attack.mitre.org/software/S0567/
- **Lazarus threat group information:** https://attack.mitre.org/groups/G0032/

How K logix Can Help

- Technology Advisory
  - Tools mitigating phishing attacks & malware analytics
  - Endpoint detection
  - Security awareness automation
- Programmatic Advisory
  - Initial build out of the security awareness program
  - Threat Intel program

ToneShell, ToneIns, and Pubload (source of graphic below) https://www.bleepingcomputer.com/news/security/chinese-hackers-use-google-drive


Send
Download
Decompress/
Unzip
ToneIns
ToneShell
PubLoad
1
2
Threat actor sends spear-phishing email with an embedded link
Spear-phishing email with a Google or Dropbox link
Malicious archive with malware
Malicious DLL sideloaded by a legitimate executable
Add a registry run key or create a scheduled task

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.