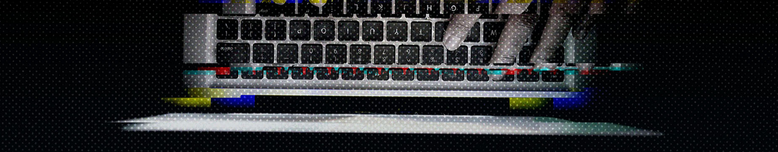
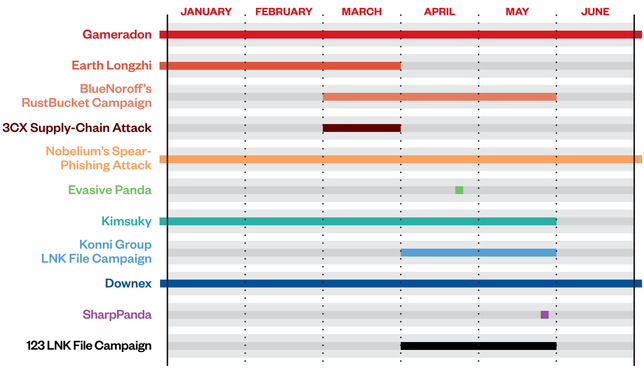


STEPPING AHEAD OF RISK

TREND MICRO 2023 MIDYEAR CYBERSECURITY THREAT REPORT

APT CAMPAIGNS

APT Campaigns



Timeline of APT campaign attacks (January – June 2023)

Notable Insights

Gameradon

2020 - present

- Targets government organizations in Ukraine
- Is delivered by spear-phishing emails, typically by attaching Word files that trigger remote template injection and execute a malicious macro
- Is possibly a general intelligence operation against Ukraine

Bluenoroff's RustBucket Campaign

March - May 2023

- Targets crypto assets and blockchain-related organizations
- Possibly aimed to obtain funds for weapons development (based on a report by the Panel of Experts of the UN Security Council Sanctions Committee)

NOBELIUM's Spear-Phishing Attack

January 2022 - present

- Targets diplomatic agencies
- Sent spear-phishing emails to diplomats and impersonated embassies in European countries
- Attached a PDF file or had an email body that contained an embedded link to the next stage payload source
- Possibly aimed at finding information on the diplomatic policies of each target country

Kimsuky

2013 - May 2023

- Targets security, diplomacy, defense, and Korean-language support groups
- Is delivered in a phishing email with a .doc and a .chm file infecting the device with a piece of malware that harvests credentials
- Collects intelligence from diplomatic, security, and national defense organizations

Downex

2022 - present

- Targets diplomatic missions and organizations in Afghanistan, Germany, and Mongolia
- Is delivered by executing a disguised .exe file that itself executes a .hta file and attempts to obtain and execute the next stage payload from the command-and-control (C&C) server
- Is possibly a general intelligence operation against the Central Asian region

Earth Longhzhi

December 2022 - March 2023

- Targets government, healthcare, technology, and manufacturing organizations
- Abuses a Windows Defender executable to perform DLL sideloading
- Disables security products by "stack rumbling" via Image File Execution Options

3CX Supply-Chain Attack

March 2023

- Targets cryptocurrency companies and users
- Uses an MSI package compromised with trojanized DLLs and a malicious macOS DYLIB
- Steals information, such as browser data and history, and launches additional attacks if the victim organization is valuable

Evasive Panda

April 26, 2023

- Targets China-affiliated individuals and individuals affiliated with NGOs in Hong Kong, Macau, and Nigeria
- Is distributed via software updates for legitimate applications
- Reportedly used backdoor MgBot

Konni Group LNK File Campaign

April - May 2023

- Targets Korean-language businesses
- Uses LNK files and tax-related decoy files in its attacks
- Is possibly motivated by monetary goals

SharpPanda

May 28, 2023

- Targets government agencies in Europe, United States, and Asia
- Is distributed by a decoy file that is a malware executable via the RoyalRoad exploit
- Is possibly a general intelligence operation against the Central Asian region

Group 123 LNK File Campaign

April - May 2023

- Targets individuals assumed to have expertise in the Democratic People's Republic of Korea (DPRK)
- Uses LNK files that infect victims with ROKRAT in its attacks