SEPTEMBER 2021

# Threat Hunter Intelligence Report

# E-Crime

splunk>
turn data into doing™

**The Threat Hunter Intelligence Report is a monthly series brought to you by Splunk's threat hunting and intelligence (THI) team. We research and produce actionable reports on the latest cybersecurity threats and trends — helping organizations stay one step ahead of adversaries, one report at a time.**

# E-crime 101

E-crime — financially-motivated cybercrime — is quickly on the rise, outpacing state-sponsored activity to account for more than 80% of interactive intrusions. Reports indicate that malware increased by 358% and ransomware by 435% in 2020. This influx of malicious attacks is projected to cost organizations a hefty $6 trillion in 2021 — reaching $10.5 trillion annually by 2025.

Today, cyber thieves are finding new, insidious ways to separate victims from their money and valuable assets. On the ransomware front, they're evolving their approach from data encryption to data exfiltration, while others are executing double extortion attacks that leak sensitive, proprietary or embarrassing data if their payment demands aren't met.

E-criminals have no qualms about exploiting the pandemic for financial gain with tactics like COVID-19 phishing and video conferencing scams as well as malicious tools like Android apps that download the CovidLock ransomware onto victims' smartphones. As for targeted industries, e-crime has sharply increased in the manufacturing sector. A rise of attacks in the healthcare, food and beverage industries suggest that bad actors are shifting focus to industries that have been hit hard by the pandemic's economic impact.

Our latest issue looks at the driving forces behind the uptick of e-crime, the tools, techniques and procedures (TTPs) e-criminals use, and where CISOs should focus their efforts to keep their customers and data safe.

## THI profile 1

# APT27 turns to ransomware during the pandemic

Deploying malware for financial gain is nothing new. There's a name for it: ransomware. But holding people's data for ransom during a pandemic is a growing trend. APT27, or Emissary Panda, was believed to be using ransomware for financial gain during the peak of the COVID-19 outbreak in China.

The group was identified by its use of extremely strong code and TTPs that were similar to their past attacks. What particularly stood out from this incident was the encryption of core servers using Bitlocker, a full volume encryption feature included in Microsoft Windows. This was unusual, since threat actors typically deploy ransomware to targeted machines, not with local tools.

### What you need to know:

APT27 is a nation-state-sponsored threat group from China known for cyber espionage and data theft. While using ransomware for financial gain is unusual behavior for this group, the peak of the pandemic may have been a catalyst for this sudden change in behavior.

## THI profile 2

# Lebanese Cedar attacks telecoms and ISPs, but not for money

Lebanese Cedar is a Hezbollah-affiliated hacker collective focused on espionage thought to be last active in 2015. But as with APT27, the pandemic brought them out of hibernation, and they've got some new tricks.

The group carried out attacks on telecommunications and internet service providers (ISPs), mostly in the Middle East, but also attacked one British and three American organizations. Lebanese Cedar used open-source tools to scan for unpatched Atlassian and Oracle servers and then deployed exploits to gain access to the servers and install web shells for future access.

This attack was unique in that it wasn't financially motivated. Instead, Lebanese Cedar was driven by political and ideological interests, targeting individuals, companies and institutions that could help the group gain political favor.

### What you need to know:

The SolarWinds attacks highlighted the growing threat to cloud and IT service providers. Because Lebanese Cedar is an espionage-based APT whose first attack in years targeted various IT and telecom organizations, their resurgence is a cause for concern. This latest attack may be a shift in behavior, but not in targeting.

## THI profile 3

# Ransomware attackers turn up the heat by targeting email

A ransomware collective known as Clop found a unique way to put pressure on its victims. The group carried out traditional ransomware attacks against target organizations then emailed the targets' customers, threatening to release their private data unless the primary targets agreed to pay the ransom. In one series of attacks, the group targeted several universities and deployed this double extortion tactic to exert maximum pressure over its victims, publishing screengrabs of personal data it claimed to have stolen, including passports, home addresses, immigration status and tax documents, and and threatened to release more if the universities didn't pay up.

### What you need to know:

Clop has used this tactic to target a range of victims, from banks and universities to maternity clothing online retail stores. Some of the emails customers reported receiving had subject lines such as "Your personal data has been stolen and will be published" and contained threats to disclose credit card details, social security numbers and other sensitive information.

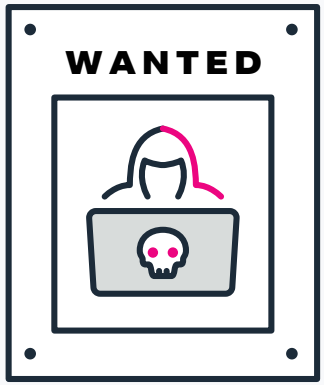
## Hacker profile

# Emissary Panda

Emissary Panda is a Chinese nation-state hacker collective that is also known as Threat Group-3390, Bronze Union, APT27, Iron Tiger and LuckyMouse. The group has been active since at least 2010 and is known for using ransomware, cyber espionage and data theft to target its victims mainly in the aerospace, government, defense, technology, energy and manufacturing sectors.

Emissary Panda became infamous for cyber espionage and data theft, and was not previously known to be financially motivated. That changed when it carried out a series of ransomware attacks during the COVID-19 pandemic lockdown in China.

Security experts linked the ransomware attacks to Emissary Panda through the pattern of TTPs used in the hacks. The group used both custom malware and readily-available tools to target mostly gaming companies, using the Windows data protection tool BitLocker to lock the servers.




**Actor type:**

Nation state, state-sponsored

**Suspected country of origin and support:**

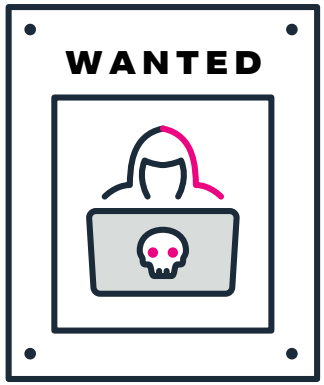
China

**Motivation:**

Espionage and data theft, and recently suspected to also be financially-motivated

# Emissary Panda

## Adversary vitals




**Targeted sectors:**

- Governments
- Aerospace
- Energy
- Gaming companies
- Defense
- Manufacturing
- Technology

**Commonly exploited technologies:**

- Bypass user account control
- Local account
- Web protocols
- Archive via library
- PowerShell
- Data from local system
- Local data staging
- Drive-by compromise
- DLL search order hijacking
- Disable Windows event logs
- Modify registry
- Network service scanning
- Obfuscated files or information

## Go phish

# FireEye


Some attackers cast a wide net to ensure their phishing campaigns are successful. Security research firm FireEye recently discovered a series of phishing attacks by a group identified as UNC2529 that targeted at least 28 different organizations across the globe, but primarily in the U.S. The attackers sent phishing emails from 26 unique addresses linked to the domain tigertigerbeads[.]com that contained malicious links designed to trick users into clicking on them. Researchers tracked the links to at least 24 different domains.

Users who clicked on a malicious link were given a PDF file that contained a heavily obfuscated JavaScript downloader. FireEye identified at least three unique strains of malware tied to the phishing attacks. The hackers disguised their attacks by using PDF documents from legitimate websites, then corrupting them by removing bytes to make them unreadable with a standard PDF viewer.

The campaign, first discovered in December 2020, mutated over recent months. PDF files were eventually replaced with Excel files with an embedded macro that, when opened, downloaded a second-stage payload. To make the emails even more convincing, the attackers tailored sender email addresses and subject lines for each victim.

# Looking for trouble?

Stay ahead of current and emerging threats by subscribing to our monthly updates on threat hunting and investigation.

**Subscribe Now**

splunk> turn data into doing™



21-18894-Splunk-THI E-Crime-EB-105