Lazarus APT Spinoff Linked to Banking Hacks

By Michael Mimoso

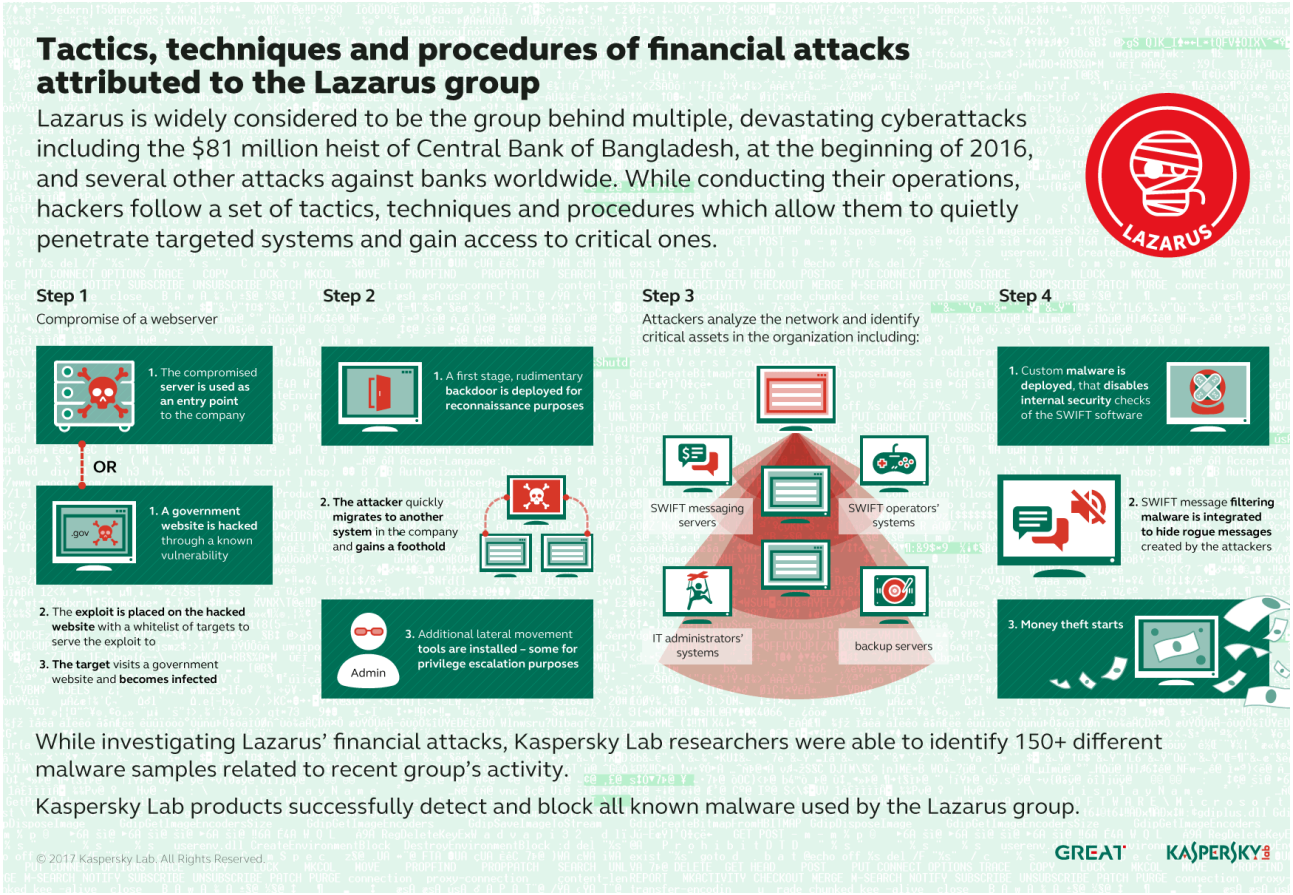
Published: 2017-04-03 · Archived: 2026-04-05 13:44:25 UTC

The Lazarus Group has splintered off a group whose mission is to attack banks and steal money in order to fund its operations.

SINT MAARTEN—The Lazarus Group, a nation-state level of attacker tied to the 2014 attacks on Sony Pictures Entertainment, has splintered off a portion of its operation to concentrate on stealing money to fund itself.

The group, widely believed to be North Korean, has been linked to a February 2016 attack against the Bangladesh Central bank that resulted in more than $850 million in fraudulent SWIFT network transactions, $80 million of which still has not been recovered.

At the Security Analyst Summit, researchers from Kaspersky Lab and BAE Systems explained how the splinter group, known as Bluenoroff, has almost exclusively hit financial institutions, casinos, financial trade software development companies and cryptocurrency businesses. The group has also been connected to an attack earlier this year against banks in Poland, based on code strings and wiper malware discovered and known to be part of Lazarus' arsenal.



Vitaly Kamluk of Kaspersky Lab and Adrian Nish and Sergey Shevchenko of BAE Systems today published an update on Lazarus and Bluenoroff, pinning to them their unique interest in SWIFT software. SWIFT is a global network supporting financial transactions and messaging between institutions. The attackers, researchers said, aren't looking for smash-and-grab bank robberies. They learn the inner workings of SWIFT software and develop and implement patches that allow the attackers to steal significant amounts of money without leaving a trace behind on the hacked systems.

Dries Watteyne, SWIFT head of customer security intelligence, also appeared at SAS and said the attackers had intimate knowledge of how the SWIFT network processes transactions and messages between financial institutions.

"They had sophisticated knowledge on a business level," Watteyne said. "They were able to make sure all messages sent from the bank and statements from the U.S. bank were hidden."

Watteyne explained that with an international transaction of U.S. dollars, emitters send payment instructions to a U.S. bank, which remits an acknowledgement before sending funds to an offshore bank.

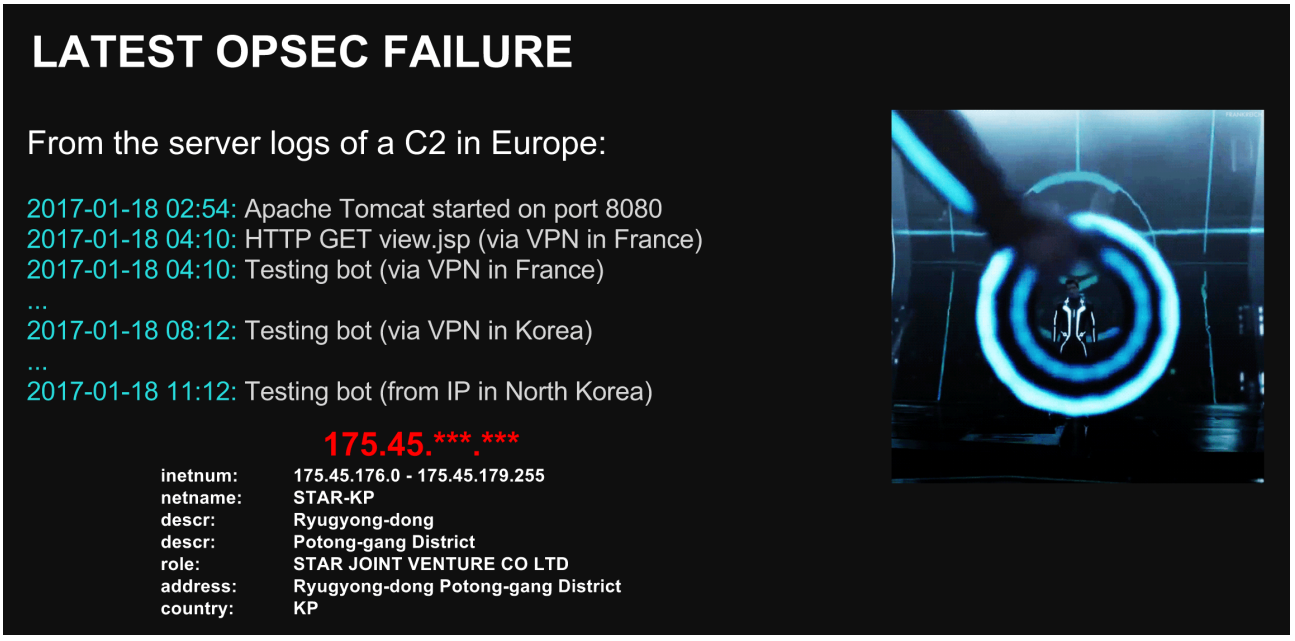
The attackers used stolen credentials to inject custom malware at the bank that was able to delete all payment instructions from the targeted database, modify SWIFT messages, including start- and end-of-day statements, and also bypass integrity verification checks built into the system.

The Lazarus Group is alleged to have leaked mountains of sensitive data from Sony Pictures Entertainment in 2014, including emails, movie scripts and other confidential information. Following the Sony hack in January 2015, the U.S. levied sanctions against North Korean defense agencies, two other government agencies and 10 individuals. The Executive Order explaining the sanctions came two weeks after North Korea suffered a DDoS attack that disconnected much of the country from the Internet.

Lazarus Group's interest in profit is relatively new, the researchers said. They've adopted a number of tactics preferred by cybercriminals, including watering hole attacks to compromise financial targets. In these attacks, a website of common interest to the target is attacked and spiked with malicious code designed to exploit a vulnerable browser or piece of third-party software.

BAE's Nish said they used iframes to redirect browsers to sites hosting scripts that check for vulnerabilities, deliver exploits and payloads. Most of the Bluenoroff attacks were initially focused on Southeast Asia and developing countries. Starting with the Poland attacks, their bravado grew and was much more global.

The link between Bluenoroff, North Korea and Lazarus gained steam, Kamluk said, from an analysis of a command and control server in Europe used in attacks. The researchers determined how the attackers connected to the server and tested their backdoors using multiple IPs from around the world. One short connection, however, was made from an IP range in North Korea.



Kamluk said the attackers' installation of cryptocurrency mining software crashed the server and likely kept the attackers from properly wiping their traces. While none of the researchers would commit fully to attributing North Korea to these attacks, the evidence does indicate some involvement.

"If it is North Korea," Kamluk said, "we know very little about its current motivation and use of offensive capabilities."

KASPERSKY lab SECURITY ANALYST SUMMIT
BlackBerry TALOS pwc Qintel Microsoft
ThreatBook CARBONITE hackerone ALIEN VAULT the DIGITRUST group SKYTEAM
BMW Motorrad SECURITY WEEK INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS AIRFRANCE KLM TRANSPORTEURS OFFICIELS OFFICIAL CARRIERS threatpost

---

Source: https://threatpost.com/lazarus-apt-spinoff-linked-to-banking-hacks/124746/