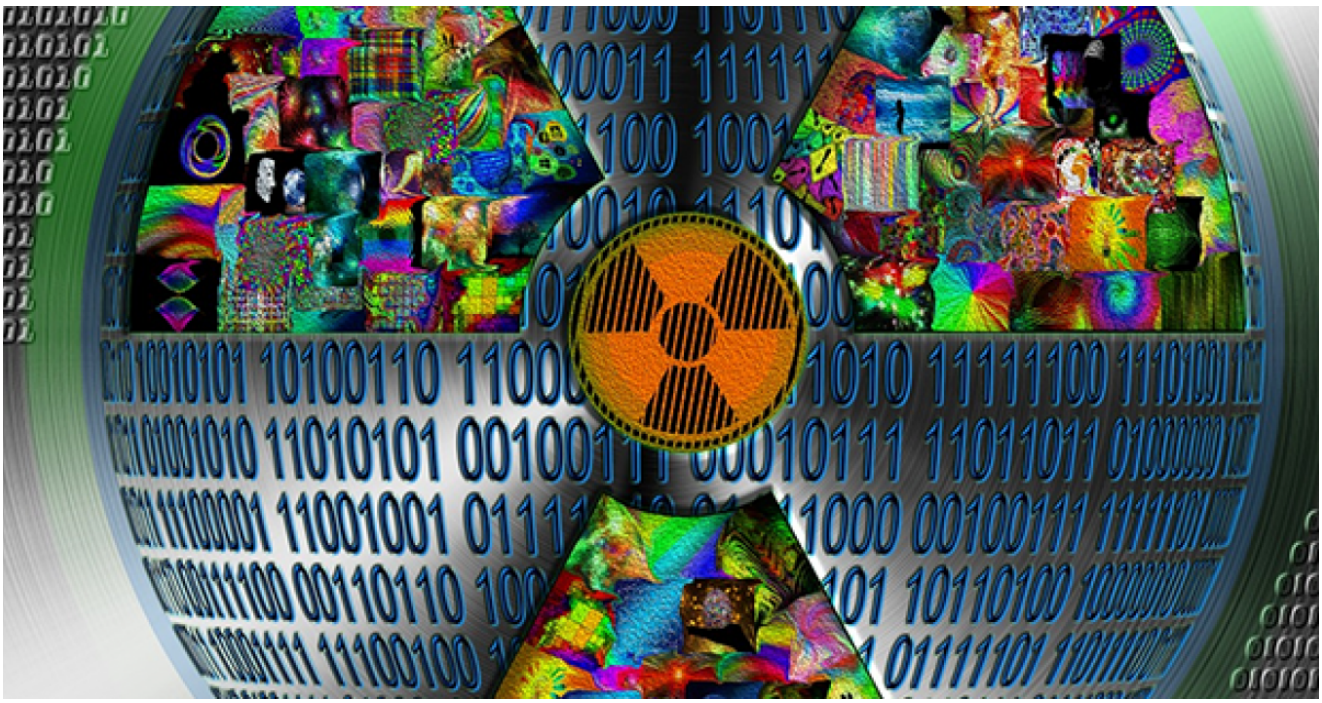
North Korea Bitten by Bitcoin Bug: Financially motivated campaigns reveal new dimension of the Lazarus Group

proofpoint.com/us/threat-insight/post/north-korea-bitten-bitcoin-bug-financially-motivated-campaigns-reveal-new

December 19, 2017



Blog

Threat Insight

North Korea Bitten by Bitcoin Bug: Financially motivated campaigns reveal new dimension of the Lazarus Group

December 19, 2017 Darien Huss

Download full report (PDF)

Overview

Proofpoint researchers have uncovered a number of multistage attacks that use cryptocurrency-related lures to infect victims with sophisticated backdoors and reconnaissance malware that we attribute to the Lazarus Group. Victims of interest are then infected with additional malware including Gh0st RAT to steal credentials for cryptocurrency wallets and exchanges, enabling the Lazarus Group to conduct lucrative operations stealing Bitcoin and other cryptocurrencies. We also discovered what appears to be the first publicly documented instance of a nation-state targeting a point-of-sale related framework for the theft of credit card data in a related set of attacks. Moreover, the timing of the point-of-sale related attacks near the holiday shopping season makes the potential financial losses considerable.

With activity dating at least to 2009, the Lazarus Group has consistently ranked among the most disruptive, successful, and far-reaching nation-state sponsored actors. The March 20, 2013 attack in South Korea, the Sony Pictures hack in 2014, the successful theft of $81 million from the Bangladesh Bank in 2014, and perhaps most famously this year's WannaCry ransomware attack and its global impact have all been attributed to the group. The Lazarus Group is widely accepted as being a North Korean state-sponsored threat actor by numerous organizations in the information security industry, law enforcement agencies, and intelligence agencies around the world.

The group has increasingly focused on financially motivated attacks and appears to be capitalizing on both the increasing interest and skyrocketing prices for cryptocurrencies. The Lazarus Group's arsenal of tools, implants, and exploits is extensive and under constant

development. Previously, they have employed DDoS botnets, wiper malware to temporarily incapacitate a company, and a sophisticated set of malware targeting the SWIFT banking system to steal millions of dollars.

In this research we detail a new implant dubbed PowerRatankba, a PowerShell-based malware variant that closely resembles the original Ratankba implant. We believe that PowerRatankba was likely developed as a replacement in Lazarus Group's strictly financially motivated team's arsenal to fill the hole left by Ratankba's discovery and very public documentation earlier this year.

We also provide a brief timeline of events related to the malicious activity and describe the various delivery methods that Lazarus Group utilized to infect victims with PowerRatankba (Fig. 1). We then detail the inner workings of PowerRatankba and how it is utilized to deliver a more fully capable backdoor to interesting victims (Fig. 1). Following that, we share details on a new and emerging threat targeting the point-of-sale industry that we have dubbed RatankbaPOS (Fig. 1). Finally, we explain our high-confidence attribution to Lazarus Group.

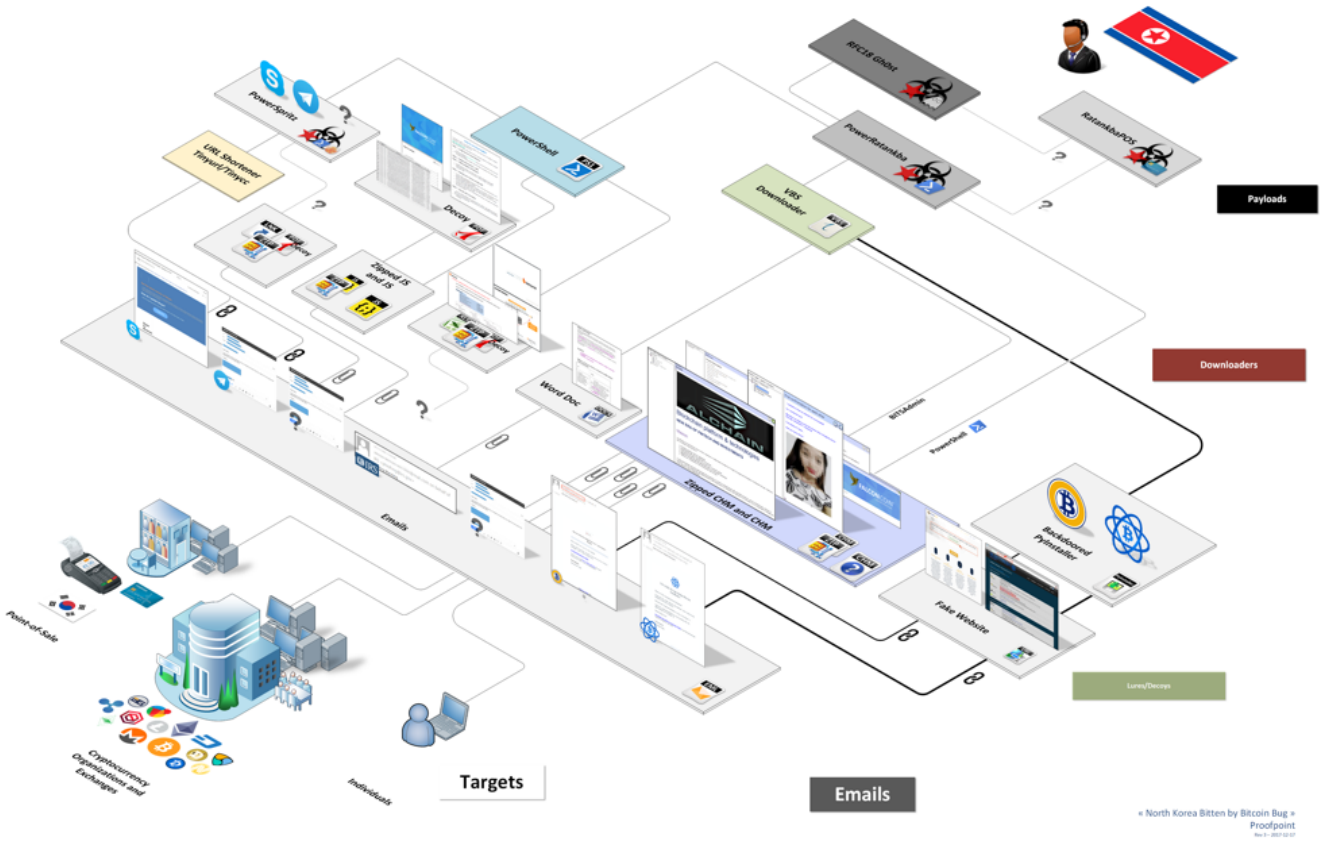


Figure 1: Flow of PowerRatankba activity from victims to the Lazarus Group operators

While this report has introduced several new additions to Lazarus Group's ever-growing arsenal, including a variety of different attack vectors, a new PowerShell implant and Gh0st RAT variant, as well as an emerging point-of-sale threat targeting South Korean devices, there are two key takeaways from this research:

- Analyzing a financially motivated arm of a state actor highlights an often overlooked or underestimated aspect of state-sponsored attacks; in this case, we were able to differentiate the actions of the financially motivated team within Lazarus from those of their espionage and disruption teams that have recently grabbed headlines.
- This group is now appears to be targeting individuals rather than just organizations:; individuals are softer targets, often lacking resources and knowledge to defend themselves and providing new avenues of monetization for a state-sponsored threat actor's toolkit.

Moreover, both the explosive growth in cryptocurrency values and the emergence of new point-of-sale malware near the peak holiday shopping season provide an interesting example of how one state-sponsored actor is following the money, adding direct theft from individuals and organizations to the more "traditional" approach of targeting financial institutions for espionage that we often observe with other APT actors.

To read more, download the full report.

Subscribe to the Proofpoint Blog