REDBALDKNIGHT's Daserf Backdoor Now Uses Steganography

blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/

November 7, 2017

APT & Targeted Attacks

REDBALDKNIGHT a.k.a BRONZE BUTLER cyberespionage group employ the Daserf backdoor in campaigns. We found that Daserf was not only used on Japanese targets, but also against other countries. We also found versions of Daserf that use steganography.

By: Joey Chen, MingYen Hsieh November 07, 2017 Read time: (words)

Additional analysis and insights by Higashi Yuka and Chizuru Toyama

REDBALDKNIGHT, also known as BRONZE BUTLER and Tick, is a cyberespionage group known to target Japanese organizations such as government agencies (including defense) as well as those in biotechnology, electronics manufacturing, and industrial chemistry. Their campaigns employ the Daserf backdoor (detected by Trend Micro as BKDR_DASERF, otherwise known as Muirim and Nioupale) that has four main capabilities: execute shell commands, download and upload data, take screenshots, and log keystrokes.

Our recent telemetry, however, indicates that variants of Daserf were not only used to spy on and steal from Japanese and South Korean targets, but also against Russian, Singaporean, and Chinese enterprises. We also found various versions of Daserf that employ different techniques and use steganography—embedding codes in unexpected mediums or locations (i.e., images)—to conceal themselves better.

Like many cyberespionage campaigns, REDBALDKNIGHT's attacks are intermittent but drawn-out. In fact, REDBALDKNIGHT has been zeroing in on Japanese organizations as early as 2008—at least based on the file properties of the decoy documents they've been sending to their targets. The specificity of their targets stems from the social engineering tactics used. The decoy documents they use in their attack chain are written in fluent Japanese, and particularly, created via the Japanese word processor Ichitaro. One of the decoy documents, for instance, was about the "plan of disaster prevention in heisei 20" (Heisei is the current/modern era in Japan).

Figure 1: File properties of one of the decoy documents that REDBALDKNIGHT sends to Japanese targets

Figures 2: Sample of decoy documents used by REDBALDKNIGHT, employing socially engineered titles in their spear phishing emails such as "disaster prevention"

Attack ChainREDBALDKNIGHT's attacks typically use spear phishing emails as an entry point. Their attachments exploit a vulnerability in Ichitaro, as shown above. These are decoy documents, often used by cyberespionage groups as a distraction while they execute their malware behind the scenes using lures such as "CPR" and "disaster prevention."

Daserf will be installed and launched on the affected machine once the victim opens the document. Daserf wasn't well-known until security researchers publicly disclosed it last year, and whose beginnings they've traced as far back as 2011. Based on the hardcoded version number they divulged (Version:1.15.11.26TB Mini), we were able to source other versions of the backdoor (listed in the appendix).

Fine-tuning Daserf Our analyses revealed Daserf regularly undergo technical improvements to keep itself under the radar against traditional anti-virus (AV) detection. For instance, Daserf versions 1.50Z, 1.50F, 1.50D, 1.50C, 1.50A, 1.40D, and 1.40C use encrypted Windows application programming interfaces (APIs). Version v1.40 Mini uses the MPRESS packer, which provides some degree of protection against AV detection and reverse engineering. Daserf 1.72 and later versions use the alternative base64+RC4 to encrypt the feedback data, while others use different encryption such as 1.50Z, which uses the Ceasar cipher (which substitutes letters in plaintext with another that corresponds to a number of letters, either upwards or downwards).

More notably, REDBALDKNIGHT integrated steganography to conduct second-stage, command-and-control (C&C) communication and retrieve a second-stage backdoor. This technique has been observed in Daserf v1.72 Mini and later versions. Daserf's use of steganography not only enables the backdoor to bypass firewalls (i.e., web application firewalls); the technique also allows the attackers to change second-stage C&C communication or backdoor faster and more conveniently.

How REDBALDKNIGHT Employs Steganography Daserf's infection chain accordingly evolved, as shown below. It has several methods for infecting its targets of interest: spear phishing emails, watering hole attacks, and exploiting a remote code execution vulnerability (CVE-2016-7836, patched last March 2017) in SKYSEA Client View, an IT asset management software widely used in Japan.

 *Figure 3: Daserf's latest execution and infection flow*

A downloader will be installed on ther victim's machine and retrieve Daserf from a compromised site. Daserf will then connect to another compromised site and download an image file (i.e., .JPG, .GIF). The image is embedded in either the encrypted backdoor configurations or hacking tool. After their decryption, Daserf will connect to its C&C and await further commands. Daserf 1.72 and later versions incorporate steganographic techniques.

REDBALDKNIGHT's use of steganography isn't limited to Daserf. We also found two of their toolkits employing the same technique—*xxmm2_builder*, and *xxmm2_steganography*. Based on their pdb strings, they're both components of another REDBALDKNIGHT-related threat, XXMM (TROJ_KVNDM), a downloader Trojan that can also act as a first-stage backdoor with its capability to open a shell. While *xxmm2_builder* allows REDBALDKNIGHT to customize the settings of XXMM, *xxmm2_ steganography* is used to hide malicious code within an image file.

REDBALDKNIGHT's tool can create, embed, and hide executables or configuration files within the image file with its tag and encrypted strings via steganography. An encrypted string can be an executable file or a URL. A threat actor will use/upload an existing image that the builder then injects with steganographic code. Additionally, we also found that the steganography algorithm (alternative base64 + RC4) between XXMM and Daserf were the same.

 *Figure 4: Code snippets showing Daserf's decode function, which is the same as XXMM's*

Figure 5: Steganography toolkit used by REDBALDKNIGHT for XXMM

 *Figure 6: Snapshots of Daserf's steganographic code generated by their toolkit*

MitigationSteganography is a particularly useful technique in purposeful cyberattacks: the longer their malicious activities stay undetected, the more they can steal and exfiltrate data. And indeed, the routine is increasingly gaining cybercriminal traction, in varying degrees of

proficiency—from exploit kits, malvertising campaigns, banking Trojans, and C&C communication to even ransomware. In the case of REDBALDKNIGHT's campaigns, the use of steganography is further compounded by their use of malware that can better evade detection and analysis.

REDBALDKNIGHT's continuous campaigns—along with their diversity and scope—highlight the importance of defense in depth. Organizations can mitigate these threats by enforcing the principle of least privilege to reduce their opportunities for lateral movement significantly. Network segmentation and data categorization help in this regard. Mechanisms like access control and blacklisting as well as intrusion detection and prevention systems help further secure the network while whitelisting (e.g., application control) and behavior monitoring help detect and block anomalous activities from suspicious or unknown files. Safeguard the email gateway to defend against REDBALDKNIGHT's spear phishing methods. Disable unnecessary and outdated components or plug-ins, and ensure that the system administration tools are used securely, as they can be misused by threat actors. And more crucially, keep the infrastructure and its applications up-to-date to reduce attack surface—from the gateways and networks to endpoints, and servers.

Trend Micro Solutions Trend Micro™ Deep Discovery™ provides detection, in-depth analysis, and proactive response to today's stealthy malware and targeted attacks in real-time. It provides a comprehensive defense tailored to protect organizations against targeted attacks and advanced threats through specialized engines, custom sandboxing, and seamless correlation across the entire attack lifecycle, allowing it to detect threats like REDBALDKNIGHT's attacks even without any engine or pattern update. Trend Micro™ Deep Security™ and Vulnerability Protection provide virtual patching that protects endpoints from threats that abuses unpatched vulnerabilities. OfficeScan's Vulnerability Protection shield endpoints from identified and unknown vulnerability exploits even before patches are deployed.

Trend Micro's suite of security solutions is powered by XGen™ security, which features high-fidelity machine learning to secure the gateway and endpoint data and applications. XGen™ protects against today's purpose-built threats that bypass traditional controls, exploit known, unknown, or undisclosed vulnerabilities, and either steal or encrypt personally-identifiable data.

A list of the Indicators of Compromise (hashes, C&Cs) related to this research is in this appendix.