Credit Card-Scraping Kasidet Leads to Detections Spike

blog.trendmicro.com/trendlabs-security-intelligence/credit-card-scraping-kasidet-builder-leads-to-spike-in-detections/

September 25, 2015

By RonJay Caragay, Michael Marcos A commercialized builder of the Kasidet or Neutrino bot, which is infamous for its distributed denial-of-service (DDoS) capabilities, have been making the rounds recently after it was leaked in an underground forum in July (version 3.6). It included a previously unheard of feature for the bot: "ccsearch" or the scraping of payment card details from point-of-sale (PoS) systems. Further investigation revealed that a paid version of the builder which included the PoS RAM-scraping feature has been around since March (version 2.9). Upon looking into the threat landscape following this discovery, we noticed that the detection count for Kasidet in June increased by 1,288% compared to the count in May. The spike in June is likely a result of cybercriminals who initially paid for the bot and used the builder in March even before it was leaked in July. Looking at one of the samples detected as WORM_KASIDET.SC, we observed that the malware affects PoS terminals running Windows operating systems. Network shares is one way for the malware to end up on PoS machines. Beause of this, networks with relatively weak security measures, such as those used by small and medium businesses (SMBs), are potentially at risk. Apart from allowing cybercriminals to scan for credit card information and have stolen data sent over a command-and-control (C&C) server, Kasidet can also launch distributed denial-of-service (DDoS) attacks, log keystrokes, copy clipboard data, and capture screenshots, execute a remote shell, and infect removable drives and network folders. Detection counts related to Kasidet are highest in Japan (12.75%), followed by United Kingdom (10.78%), Taiwan (7.84%), and France (6.86%).

Figure 1. Country distribution of Kasidet detections, July 1 – September 17, 2015

Multiple Arrival Vectors The version of the builder leaked in the underground forum *nulled[dot]io* was already cracked, thus offering a free tool that cybercriminals can use to

steal payment card details from PoS systems. The builder and control panel of the latest version of BKDR_KASIDET.SM, was uploaded by a user nicknamed “0x22.” Copies of the builder package have been replicated in other hacker forums like *hackforums[dot]net* and *crimebiz[dot]net*.

Figure 2. Screenshot of most recent version of Kasidet builder with PoS RAM scraper leaked in underground forum

Figure 3. Screenshot of cracked Kasidet builder (version 3.9.4) with PoS RAM scraper

Apart from the forum, we have also observed this variant using different arrival vectors such as exploit kits, spammed emails, removable drives, networks, and as payloads of other Trojans. For example, we found a variant, BKDR_KASIDET.FD, being sent over spammed messages.

Figure 4. Sample spammed message containing BKDR_KASIDET.FD

Another variant, WORM_KASIDET.NM, was observed to be delivered as the final payload for the Sundown exploit kit. Cybercriminals using this worm can use the backdoor command "ccsearch" to run PoS RAM scraping routines on affected machines. ***Old Malware, New Money*** This is not the first time that memory-scraping capabilities were added into a botnet tool like Neutrino. PoS-specific features of the FighterPoS code were built on top of malware that was designed for botnets. However, the upgrade of Kasidet to include memory-scraping functions is still quite notable. Upgrading old malware to include PoS RAM-scraping capabilities is a new technique in the threat landscape, but it’s not surprising given how lucrative stolen payment card data is. It shows that more and more cybercriminals are putting two and two together to make more money. PoS RAM scrapers are usually sold underground at a price at par with their lucrative potential and now that cybercriminals have access to a cracked version of a memory-scraping botnet tool, they can conduct attacks without the hassle of paying excessively for it. Scoring this tool is basically finding a valuable tool in a bargain bin and ending up not having to even pay for it. ***Notable Routines*** Apart from its card-scraping capabilities, the malware checks the following to evade detection:

- Which virtualization modules (BOCHS, QEMU,VBOX,VMWARE) are loaded
- if a debugger is present
- if the system's username and path name is related to a sandbox system
- if registries contain virtualization-related keys
- and the window class name

Another notable behavior of Kasidet is that its C&C servers return a "404 Not found" error code, but in fact contain its base-64 encoded commands below the error page.

Figure 5. Screenshot of "404 Not found" error code sent by Kasidet C&C

It can also inject browsers and FTP client servers to monitor network activities. It also checks registry keys related to Microsoft email clients to gather email credentials. ***Solutions*** Trend Micro protects customers from all threats related to Kasidet. To protect enterprises from bots and malware with PoS RAM-scraping capabilities, it is best to employ endpoint application

control or whitelisting technology, included in the Trend Micro Smart Protection Suite, to keep you in control of the applications that run on your network. Enterprises can also consider Trend Micro Deep Discovery, which has specialized detection engines and custom sandboxing that can detect evasive attacker activities like the anti-sandboxing techniques mentioned in this entry. ***With additional information by Sylvia Lascano.*** *Updated on September 29, 2015 12:10 P.M. PDT (UTC-7) to add related Trend Micro solutions.*

Content added to Folio

Malware

By: Trend Micro September 25, 2015 Read time: (words)