TrendLabs SECURITY INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Backdoor as a Software Suite: How TinyLoader Distributes and Upgrades PoS Threats

- Posted on:May 10, 2016 at 3:07 pm
- Posted in:Malware
- Author:
  Erika Mendoza and Jay Yaneza (Threats Analysts)

0

On their own, a multicomponent backdoor and a point-of-sale (PoS) malware can pose great threats to enterprises and small and medium-sized businesses (SMBs). As a tandem, these two can lead to stealthier and more flexible attacks. But add *another* PoS malware to the mix, and you've got even bigger trouble.

TinyLoader, AbaddonPOS, and TinyPOS are doing just that, infecting systems in Europe and North America. TinyLoader, a backdoor known for infecting systems with other malware, was first seen distributing AbaddonPOS PoS malware around November 2015. When we noticed a sudden spike in AbaddonPOS detections just this January, TinyPOS, another PoS malware strain, has also reared its ugly head that time. Our analysis suggests that these two PoS threats are related, and not only in terms of how they are distributed and upgraded. We surmise that the operators behind these two seemingly separate PoS threats are one and the same.

The role of TinyLoader

To figure out if AbaddonPOS and TinyPOS are indeed connected, we looked at what they had in common—TinyLoader. This backdoor is a known means for introducing secondary infections to systems. Note though that it is not the primary or sole indicator of PoS malware infection.

TinyLoader has two small components—a screen grabber and a process enumerator. These modules are used to gather information or reconnaissance on infected systems. After TinyLoader diagnoses an infected system, it chooses the aRppropriate payload to deliver to the machine.

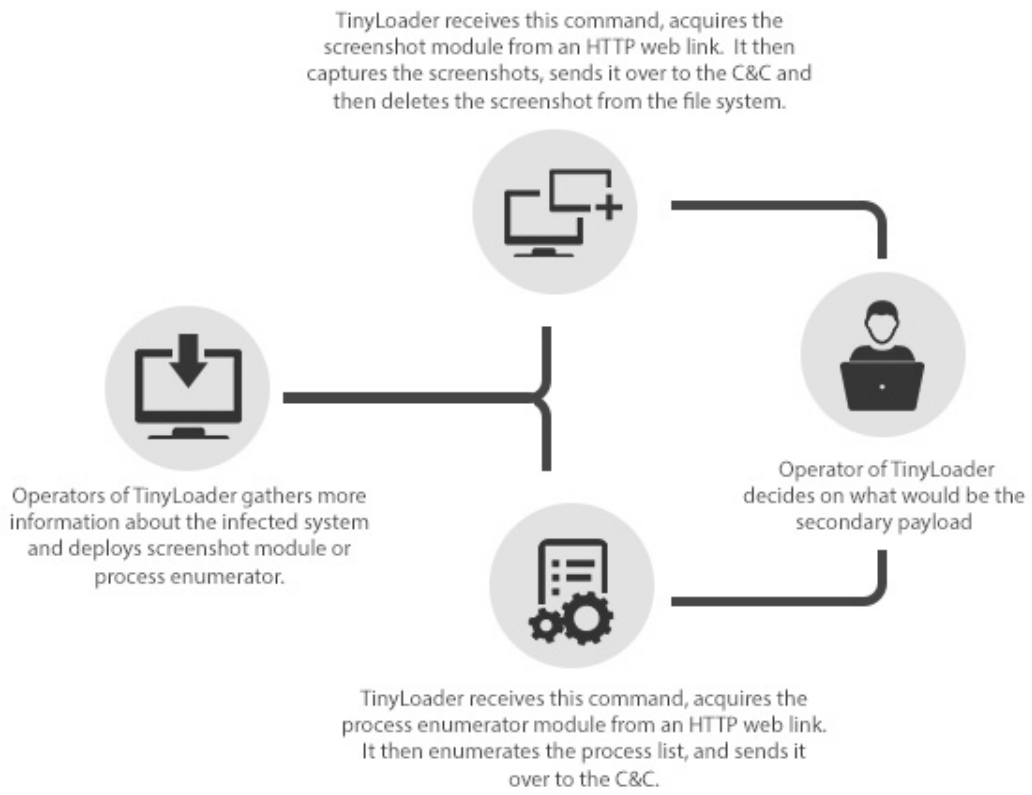

Figure 1. TinyLoader uses two components for reconnaissance

As has been said, TinyLoader started distributing AbaddonPOS variants in November 2015. We have been detecting AbaddonPOS variants as BKDR_TINY, BKDR64_TINY, or TROJ_TINY. Based on our Smart Protection Network data, Asia Pacific and Europe are heavily affected by TinyLoader from the period of January-April 2016.

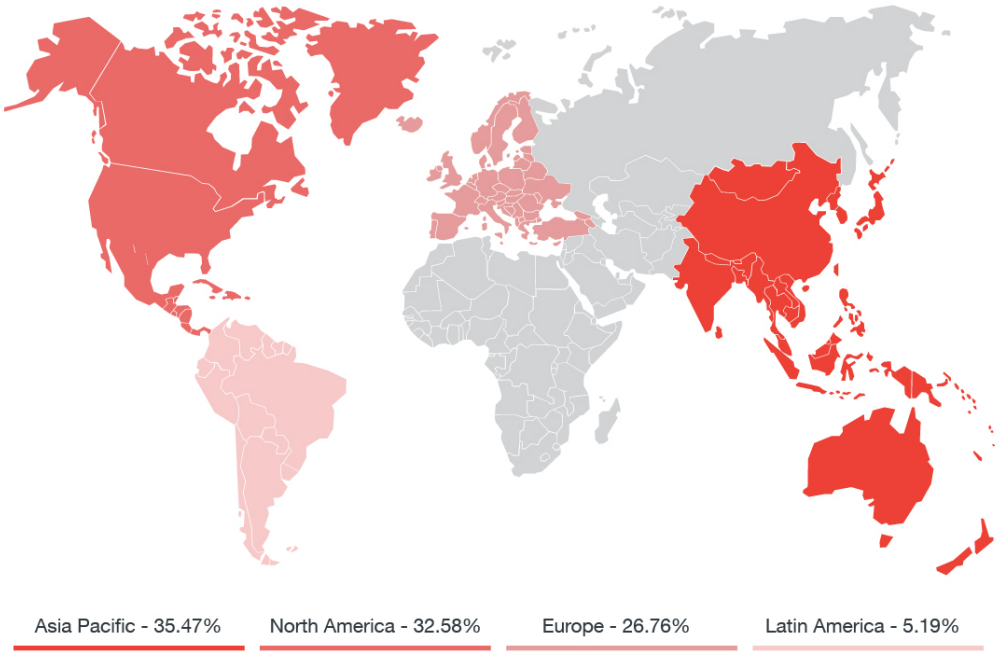

Figure 2. The number of TinyLoader-related infections from January to April 2016

Analysis also revealed that apart from spreading AbaddonPOS variants, TinyLoader also has a hand in managing the malware's upgrades. As it turns out, TinyLoader also distributes TinyPOS variants. But that is not conclusive. So we sought to further compare AbaddonPoS with TinyPOS.

We looked at how newer versions of AbaddonPOS were distributed and found that the initial versions of TinyPOS were distributed the same way. AbaddonPOS were tested first via selective deployment and only when these deployments were proven successful will they only go for wide distribution. We have yet to see a mass deployment of TinyPOS but we're already seeing infections within the United States and some parts of Europe.

Trend Micro protects customers from all threats related to TinyLoader. To protect enterprises from malware with PoS RAM-scraping capabilities, it is best to employ endpoint application control, that reduces attack exposure by ensuring only updates associated with whitelisted applications can be installed. Endpoint solutions such as Trend Micro™ Security, Trend Micro™ Smart Protection Suites, and Trend Micro Worry-Free™ Business Security can protect users systems from AbaddonPOS, TinyPOS, and TinyLoader backdoor by detecting these malicious files.

For more details on how TinyLoader serves as a software management suite for deploying and upgrading AbaddonPOS and TinyPOS, and seemingly links the two threats together, read our technical brief.

Related Posts:

- KillDisk and BlackEnergy Are Not Just Energy Sector Threats
- QAKBOT Resurges: Despite Takedowns, Online Banking Threats Persist
- Online Banking Threats in 2015: The Curious Case of DRIDEX's Prevalence
- Android-based Smart TVs Hit By Backdoor Spread Via Malicious App

Tags: AbaddonPOScybercrimePOS malwarePoS threatsTinyLoaderTinyPOS

Featured Stories

- How Bad is Badlock (CVE-2016-0128/CVE-2016-2118)?
- ATM Malware on the Rise
- Mobile Devices Used to Execute DNS Malware Against Home Routers
- Indian Military Personnel Targeted by "Operation C-Major" Information Theft Campaign
- Massive Malvertising Campaign in US Leads to Angler Exploit Kit/BEDEP

Recent Posts

- Pawn Storm Targets German Christian Democratic Union
- May 2016 Patch Tuesday Fixes Browser and Scripting Engine Flaws
- Backdoor as a Software Suite: How TinyLoader Distributes and Upgrades PoS Threats
- The Panamanian Shell Game: Cybercriminals With Offshore Bank Accounts?
- ImageMagick Vulnerability Allows for Remote Code Execution, Now Patched

Cybercrime Across the Globe: What Makes Each Market Unique?

- This interactive map shows how diverse the cybercriminal underground economy is, with different markets that are as unique as the country or region that it caters to.
  Read more

Business Email Compromise

- A sophisticated scam has been targeting businesses that work with foreign partners, costing US victims $750M since 2013.
  How do BEC scams work?

Popular Posts

Data Protection Mishap Leaves 55M Philippine Voters at Risk
New Crypto-Ransomware JIGSAW Plays Nasty Games
How Bad is Badlock (CVE-2016-0128/CVE-2016-2118)?
Mobile Devices Used to Execute DNS Malware Against Home Routers
Locky Ransomware Spreads via Flash and Windows Kernel Exploits

Latest Tweets

- Business #email compromise scam makes away with nearly $500K: bit.ly/1QX45eZ #infosec
  about 2 hours ago
- TinyLoader backdoor teams up with 2 #PoS #malware: bit.ly/1WoX3bz
  about 5 hours ago
- #Imagemagick #vulnerability, now patched: bit.ly/1rU0MQY #infosec
  about 9 hours ago

Stay Updated

Email Subscription