A TrendLabs Report

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

TrendLabs Security Intelligence Blog

Jay Yaneza and Erika Mendoza
Trend Micro Cyber Safety Solutions Team

May 2016

Contents

Introduction

The tandem of TinyLoader backdoor and a point-of-sale (PoS) threat, AbaddonPOS was first reportedly seen in 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. This prompted us to probe further on these threats and check if they are in any way related to one another.

Our analysis reveals that TinyLoader, a backdoor used for secondary malware infection, is distributing and managing the upgrades of AbaddonPOS. Likewise, TinyLoader is also spreading TinyPOS variants. This leads us to conclude that the operators behind TinyPOS and AbaddonPOS are one and the same.

In this technical brief, we'll discuss the ties that bind TinyLoader with two notorious PoS threats—AbaddonPOS and TinyPOS, including how the perpetrators behind this operation deployed their arsenals.

TinyLoader—The Not-So-Missing Link?

It's always good to examine the entry points of PoS malware in their target environment to understand these threats better. Initial information on AbaddonPOS details its links to TinyLoader backdoor, which Trend Micro detects as BKDR_TINY, BKDR64_TINY or TROJ_TINY.

TinyLoader can run any shellcode on the system and its primary function is to introduce secondary infections on the environment. That being said, seeing TinyLoader in an environment is not the leading or sole indicator of PoS threats as it can be directed to do other malicious activities. For the purpose of this write-up, we checked any indicator connecting AbaddonPOS and TinyPOS.

Based on our Smart Protection Network data, there are more TinyLoader-related infections in Asia-Pacific and North America from the period of January-April 2016. Our data also indicate that 64% of our detections on TinyLoader infections are mostly Windows 7 (64 Bit) platforms.

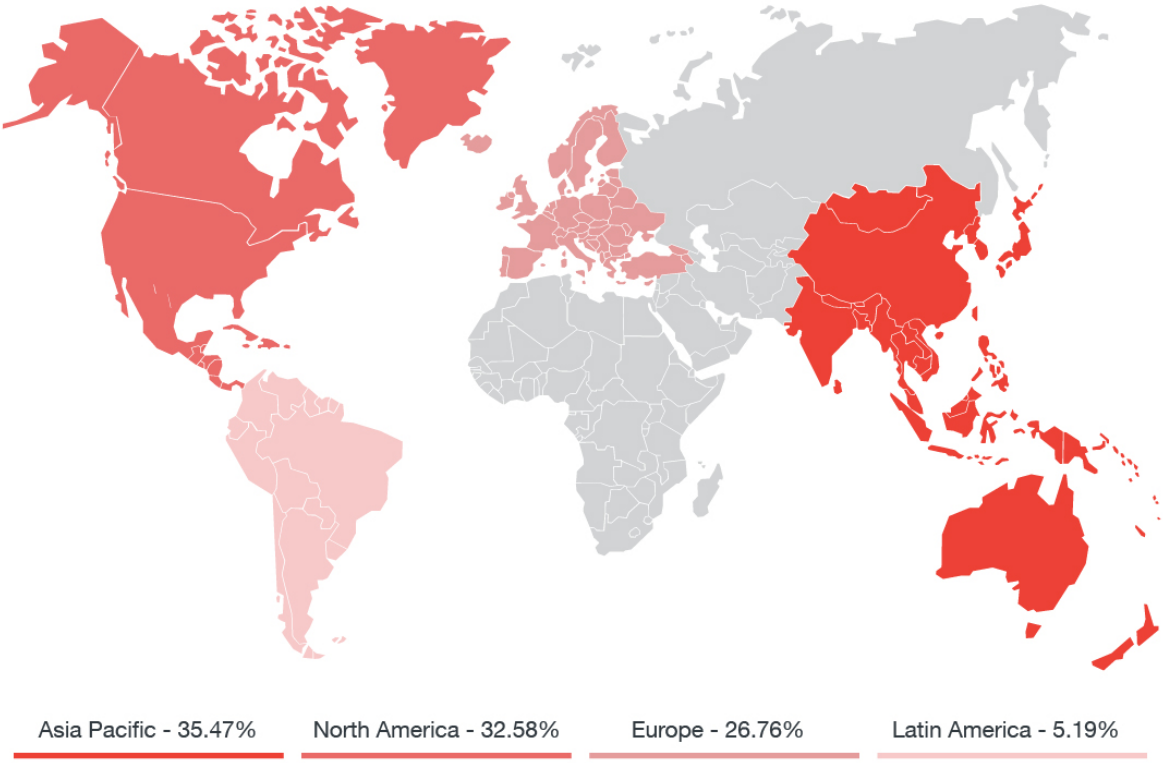

Figure 1. Global distribution of TinyLoader-related infections (January-April 2016)

Method of Operations: Testing First Before Mass Deployment

As seen in the geographical map above, there's a widespread presence of TinyLoader-related infections across the globe. With this established footprint, TinyLoader can selectively introduce secondary infections based on what's interesting in the environment it is running on. This business model is true to any malware as a service.

TinyLoader used two very small components: a module that can take a screenshot (grabber), and a module that functions as a process enumerator. Both modules are very small in size and simply loaded into memory. But these modules do not necessarily have any malicious payload. They are just used to gather information or reconnaissance on infected systems. During our research, we identified that screenshot grabber were deployed several times a day for over an extended period for collecting data on the system.

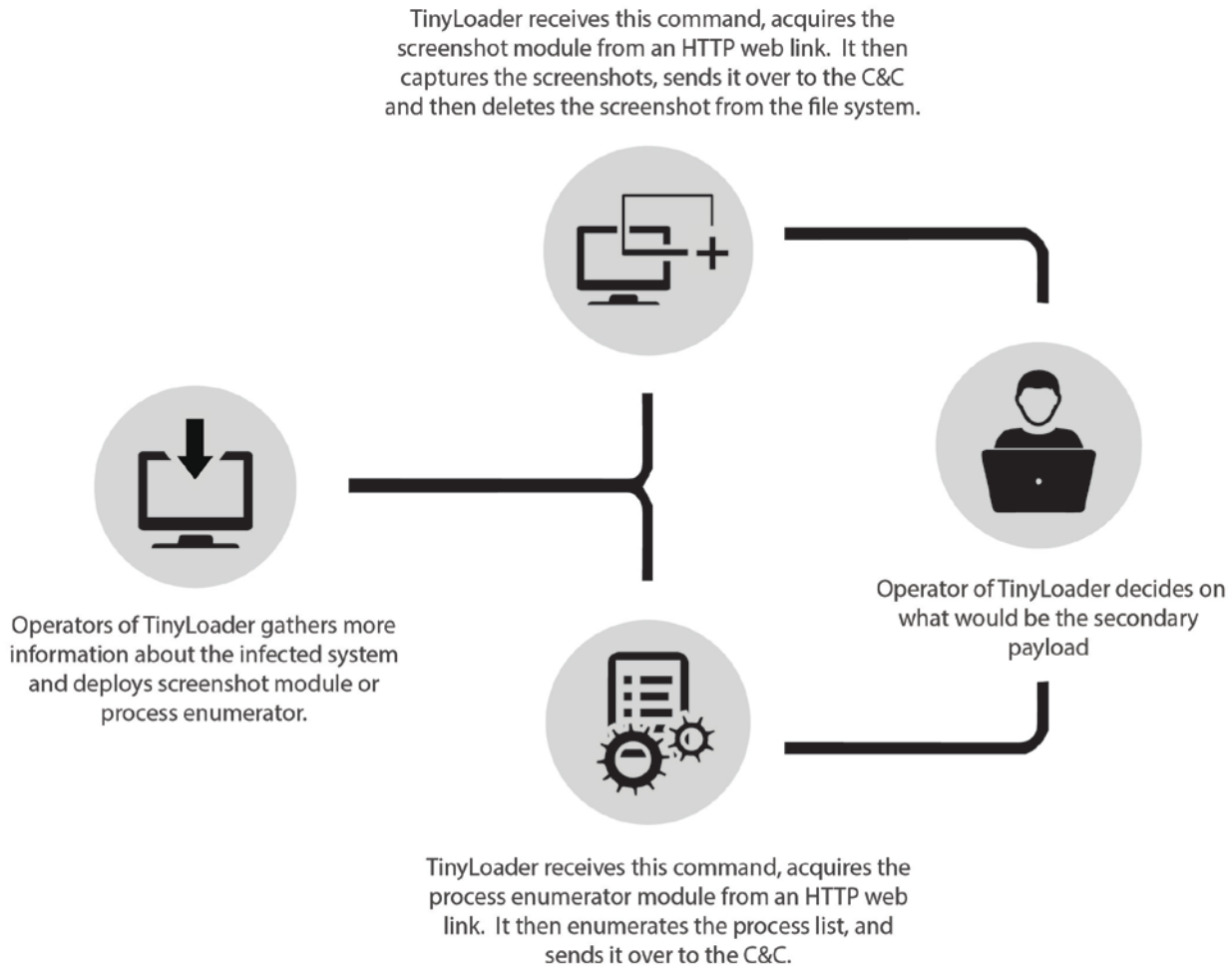

Figure 2. TinyLoader uses two small components for reconnaissance

After TinyLoader identifies an infected system, the operator then may choose to deploy a secondary payload. In this particular case, it was AbaddonPOS first, followed by TinyPOS. We have identified two periods where AbaddonPOS variants were massively distributed:

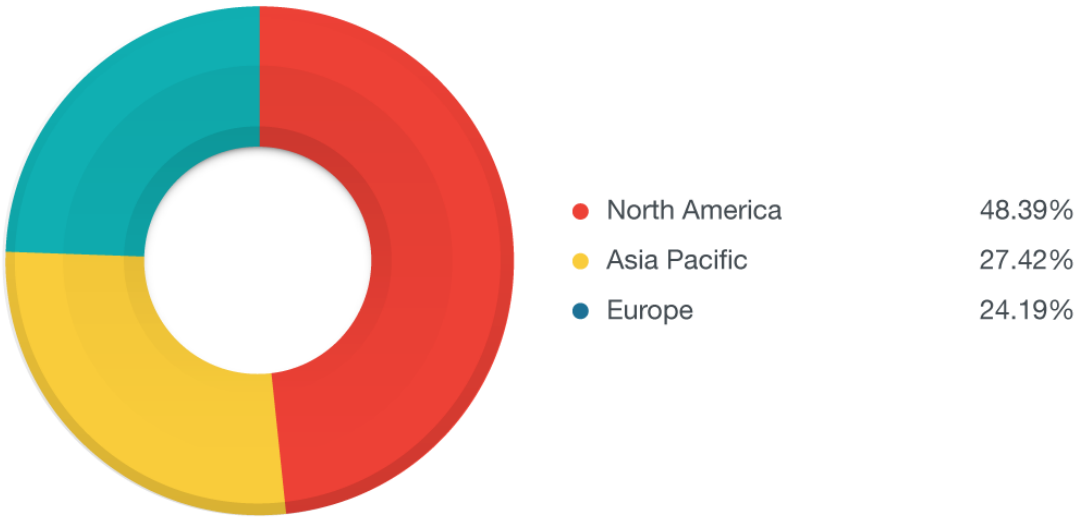

Figure 3. North America is heavily affected by the first wave of AbaddonPOS attacks, around January 29-30, 2016

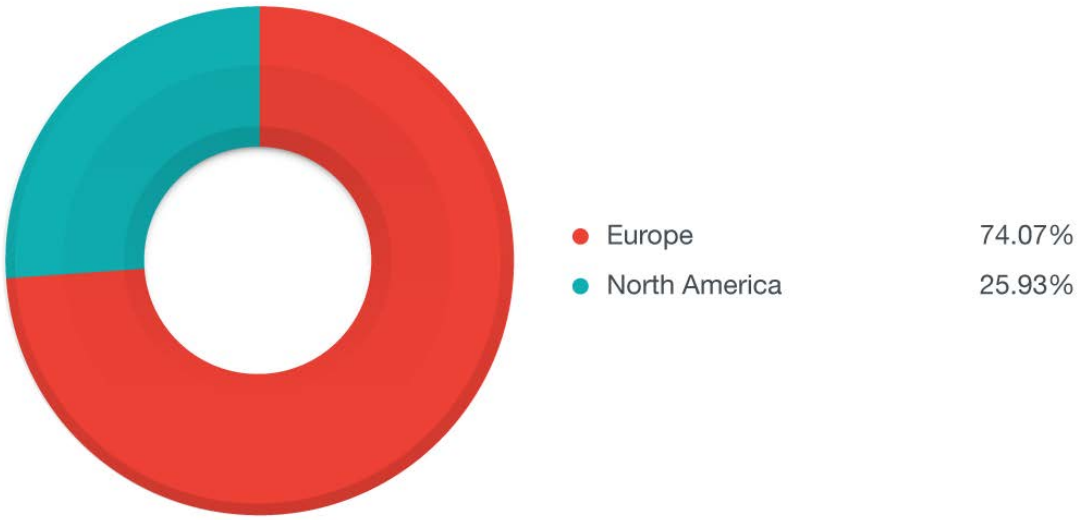

Figure 3. The second wave of AbaddonPOS attacks mostly hit countries in Europe, around March 31 – April 1, 2016

Since most of the infected environment run on Windows 7 operating system (OS), AbaddonPOS is stored in *%PROGRAMDATA%*. In its initial wave, it used the file name, *scheduler.exe* and the mutex, *MR_D*, resembling some of the documented behaviors of this PoS malware in 2015. After this initial mass-deployment, there were small incremental file variations being introduced throughout February 2016.

Around March of this year, we started seeing similar detections on *%PROGRAMDATA%* stemming from TinyLoader. However, it used a different file name—*conhost.exe*. Our analysis shows that this is still AbaddonPOS with very slight modifications. It uses now the mutex, *MR_X*. This modified version of AbaddonPOS was mass-deployed at the start of April 2016.

We also noticed a binary (Sha1: 7fd44fdcc12988cb1f0811f79ec8f41bec65800f) referencing the file names, *scheduler.exe* and *conhost.exe*. The said binary was downloaded on the same site hosting AbaddonPOS. This binary, which we dubbed as updater component, was distributed

around February 29, 2016, a month after the initial wave. The file's logic was quite simple:

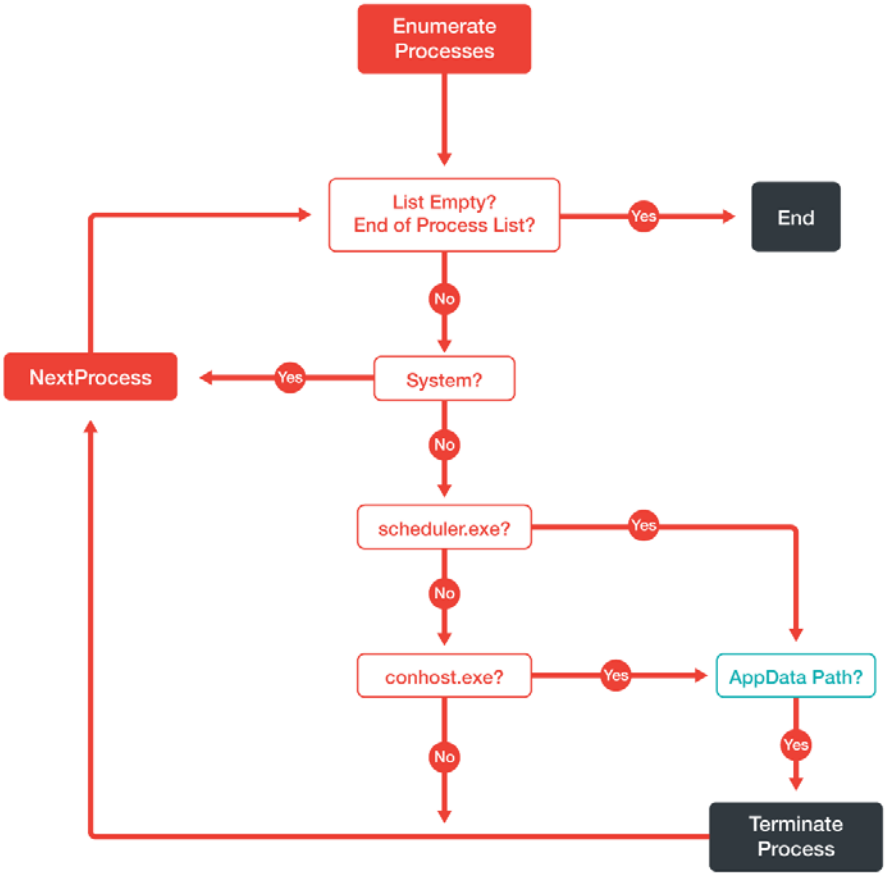

Figure 4. The update component enumerates running processes and checks for familiar file names in All User's application data folder. It then terminates these if found.

Aside from *%ProgramData%\scheduler.exe*, the updater component looks for another file, *conhost.exe* in the same directory, which seemed unusual. However, this made sense when AbaddonPOS was deployed with the file name, *%PROGRAMDATA% \conhost.exe* last March 2016. TinyLoader was preparing to upgrade the existing installations of the said PoS malware. We saw that TinyLoader not only distributed AbaddonPOS but also managed the upgrades of this PoS threat.

Ties that Bind: The TinyPOS-AbaddonPOS Connection

When a new PoS malware strain, TinyPOS emerged in threat landscape, we checked its connection to AbaddonPOS. Since TinyPOS is hosted on the same server as AbaddonPOS (see diagram below), it prompted us to dig deeper into these threats. We were able to identify that TinyLoader was distributing both PoS threats.

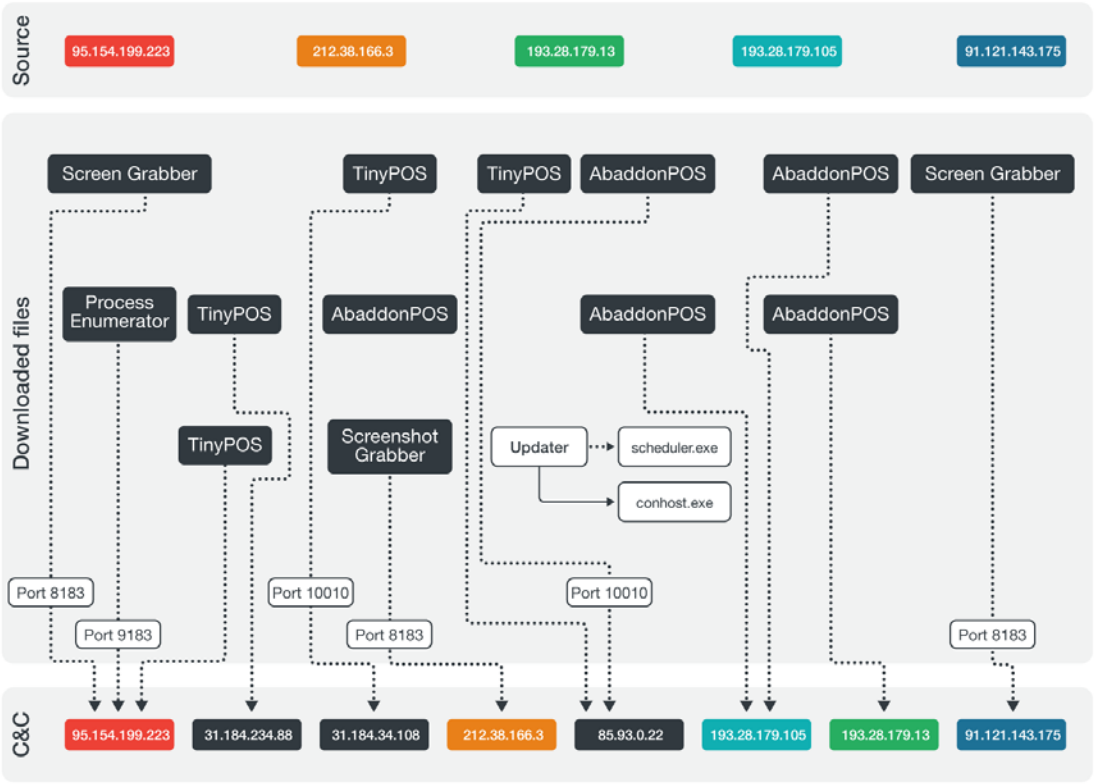

Figure 5. Mapping of file sources and C&C servers

In addition, we also saw the updater component that cleans up process names used by AbaddonPOS (*scheduler.exe* and *conhost.exe*) and TinyPOS (*wmi_service.exe*).

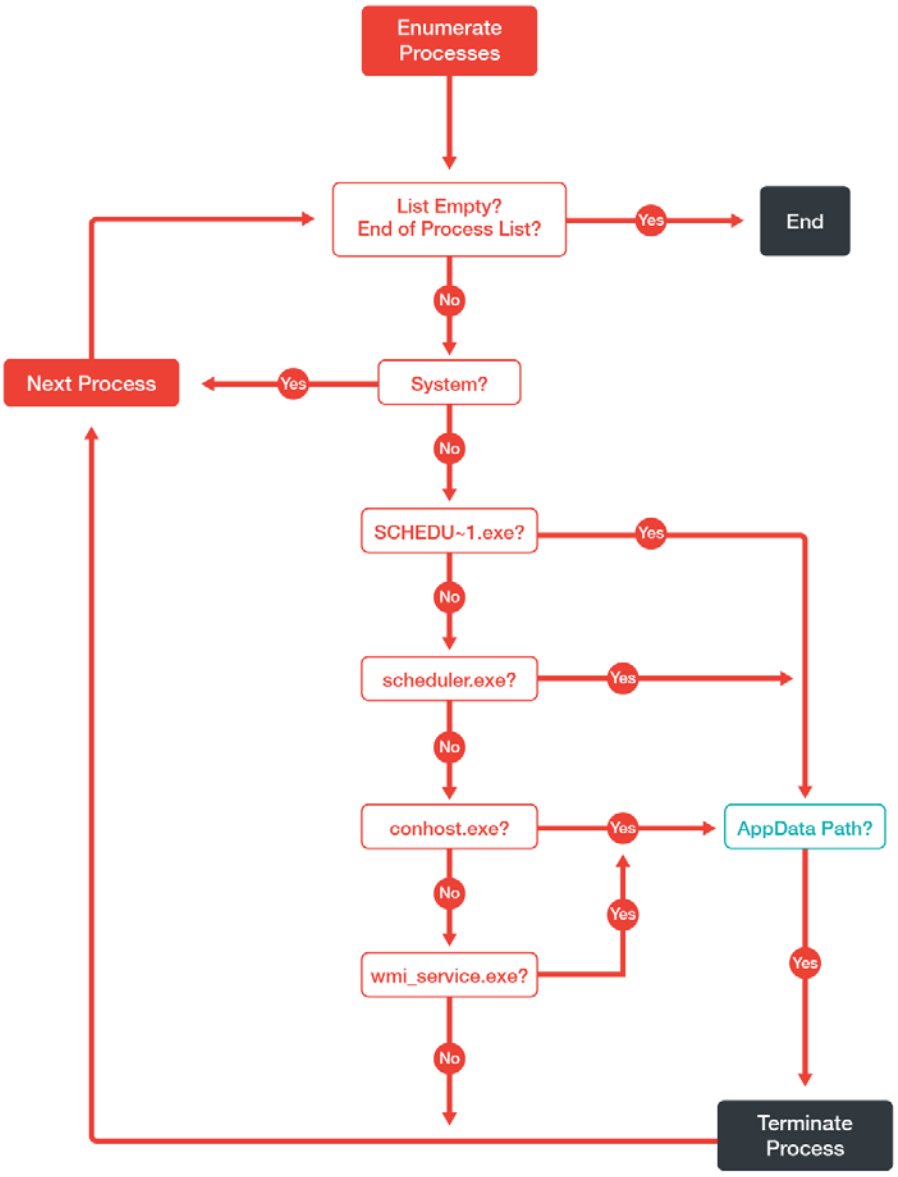

Figure 6. New updater component logic

Last April 2016, TinyPOS started sporting tactics commonly associated with PoS RAM scraper. PoS RAM scrapers usually look for process names either for exclusion (similar to what AbaddonPOS did) or for targeting. Targeting is a selective method of seeking out a known process.

In this modification or improvement (sha1: 5b65d0a2df243412f95965f5e2cd1a17676960b1), TinyPOS used a particular binary in memory: *resdbs.exe*. This binary otherwise known as MICROS ® Database Service is part of several MICROS® software solutions. Various industries like retail typically use these software solutions.

TinyPOS scans all other processes not included in the whitelist. It also creates a separate thread that only monitors the Micros service. With this dedicated thread, this malware increases its chances of capturing credit card information from the *resdbs.exe* process memory.

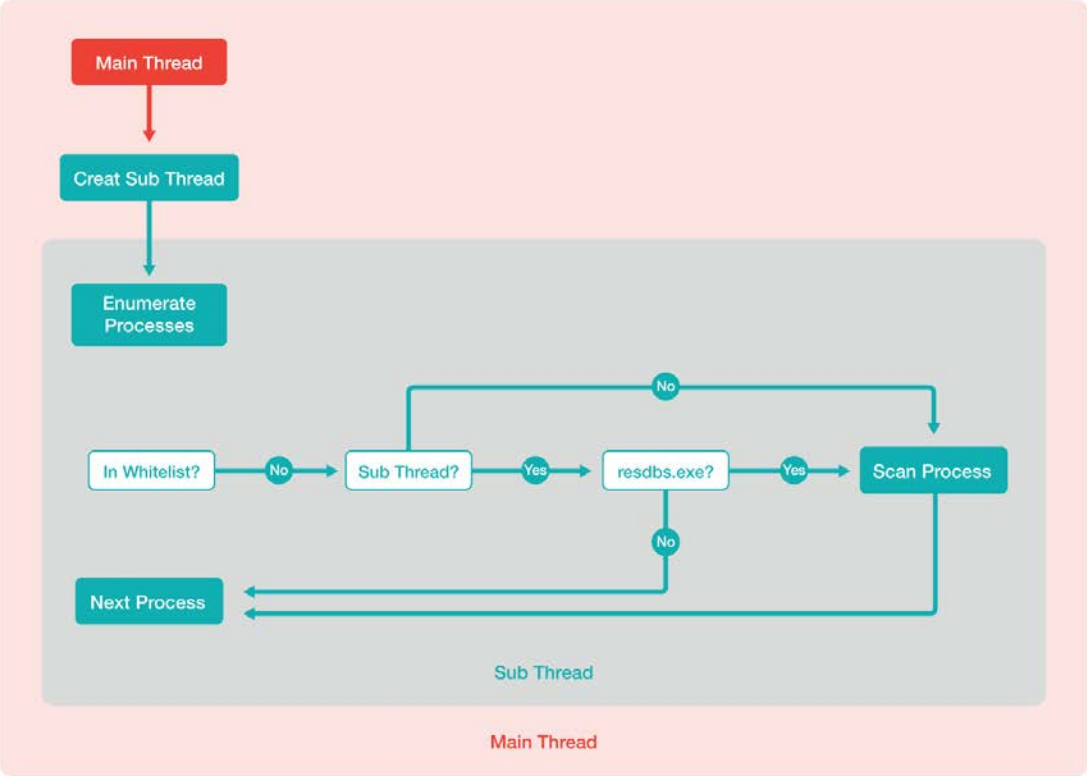

Figure 7. TinyPOS creates a separate thread dedicated to resdbs.exe monitoring.

It is also worth noting that AbaddonPOS also has a separate thread for monitoring specific processes. However, our samples show that its list is blank. The only difference between TinyPOS and AbaddonPOS in this particular context is the coding approach. It seems that TinyPOS is a simplified version of AbbadonPOS.

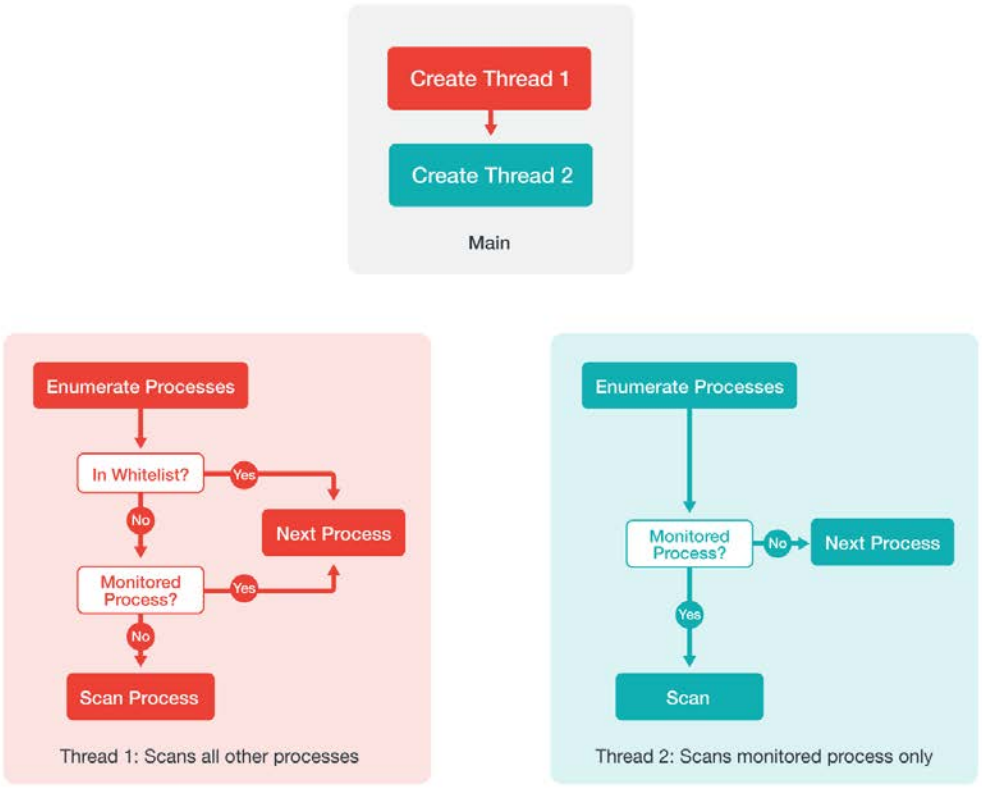

Figure 8. AbaddonPOS coding approach

Targeting PoS software components are very common. MalumPOS and RawPOS are some examples of PoS threats that employed the same technique. Both TinyPOS and AbaddonPOS modified the process list to match the target environment's point-of-sale software, similar to what RawPOS did.

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.

Widespread Distribution

Through our research, we established that AbaddonPOS and TinyPOS are one and the same PoS family. They cast a wide net to hit as many environments as possible and to prepare that environment for secondary infections. This tactic is reminiscent of another PoS threat, GamaPOS.

The combined infections of AbaddonPOS and TinyPOS have struck various industries:

- Technology
- Healthcare
- Transportation
- Education
- Manufacturing
- Fast-Moving Consumer Goods (FMCG)
- Government

This list of affected industries seems extensive but not surprising, particularly in the United States. According to a survey released by the Strawhecker Group (TSG), only 37% of US merchant locations are EMV-ready after the October 1, 2015 liability shift. The same survey also revealed that the implementation has been slower than expected. The estimated adoption rate should be at least 90% by 2017.

As merchants tried to catch up to EMV implementation, attackers are already showing a keen interest at other verticals to hit before higher adoption takes place. They (attackers) are using their malicious tools to infect as many PoS systems as possible before point-to-point encryption will be fully adopted.

When the card data is not encrypted in the reader, this makes a terminal even with Chip-and-Pin susceptible to PoS RAM scraper malware. A non-EMV enabled terminal also allows anyone who has duplicated card data (card-in-hand) to walk in an establishment and use that duplicated card. He/she can also place an online transaction where details such as the three-digit security code and billing address are not verified.

Challenges and Recommendations

On their own, a 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.

The use of TinyLoader with a PoS threat is quite effective. Its multicomponent architecture allows several small modules to be built depending on the need. This makes attacks less noticeable, thus avoiding detection. The small modules also enable the secondary infection to be successful.

The command-and-control (C&C) server of TinyLoader needs not to be a server where it gets the components. It can be directed to connect to another site for downloading the component. The downloaded component (secondary malware) can then report to its own C&C server.

As detailed above, TinyLoader was used like a software management suite to manage the deployment and upgrade of both AbaddonPOS/TinyPOS. Analyzing these samples individually would not lead to any conclusion. Acquiring only the TinyLoader executable absolutely made no sense because one has to observe how other components are being used.

This presents challenges in both static and dynamic analysis. In static analysis of TinyLoader, only a TCP socket connection to a pre-defined IP address and port is visible. In dynamic analysis (where most sandboxes can only run the sample for a few minutes), a similar raw socket connection is also seen. This means that only through actual infection can one observe the complete infection chain—from launching tools and gathering information on the system to secondary infection.

The businesses affected by this combined backdoor and point-of-sale threat were spread out between single seat infections and SMBs. TinyLoader used a high numbered port to communicate back to its own C&C server while being able to introduce additional files in the environment via HTTP requests. This spells the importance of looking into outbound requests (or traffic leaving the environment) aside from the common practice of restricting inbound and outbound requests to certain known services.

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. While Trend Micro detects all indicators that were discussed here, we still are monitoring the progression of this threat.

Appendix: Example Indicators of Compromise

SHA1	Threat
5b65d0a2df243412f95965f5e2cd1a17676960b1	TinyPOS
30D265E5471011AE8DCC196D3BB16DB6F1F1CF21	AbaddonPOS
1B64812ACA45F531AF3382677F4AFE6C1B32F2E8	TinyLoader
387d16fe19c36b30fa7752c86a825be93a8adb5e	TinyLoader screen grabber
3b9dd85a476bee26abed3366ce5e9763b4de84e4	Tiny Loader process enumerator
7fd44fdcc12988cb1f0811f79ec8f41bec65800f	TinyLoader Update module for TinyPOS/AbaddonPOS

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Securing Your Journey to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003