MajikPOS Uses PoS Malware, RATs for Malicious Tricks

blog.trendmicro.com/trendlabs-security-intelligence/majikpos-combines-pos-malware-and-rats/

March 15, 2017

Malware

We've uncovered a new breed of point-of-sale (PoS) malware currently affecting businesses across North America and Canada: MajikPOS. MajikPOS is designed to steal information, but its modular approach in execution makes it distinct.

By: Cyber Safety Solutions Team March 15, 2017 Read time: (words)

We've uncovered a new breed of point-of-sale (PoS) malware currently affecting businesses across North America and Canada: MajikPOS (detected by Trend Micro as TSPY_MAJIKPOS.A). Like a lot of other PoS malware, MajikPOS is designed to steal information, but its modular approach in execution makes it distinct. We estimate that MajikPOS's initial infection started around January 28, 2017.

While other PoS malware FastPOS (its updated version), Gorynych and ModPOS also feature multiple components with entirely different functions like keylogging, MajikPOS's modular tack is different. MajikPOS needs only another component from the server to conduct its RAM scraping routine.

MajikPOS is named after its command and control (C&C) panel that receives commands and sends exfiltrated data. MajikPOS's operators use a combination of PoS malware and remote access Trojan (RAT) to attack their targets, to daunting effects. MajikPOS is a reflection of

the increasing complexity that bad guys are predicted to employ in their malware to neuter traditional defenses.

Entry Point and Attack Chain

Feedback from our Smart Protection Network™ enabled us to determine the methods the bad guys used to illicitly gain access to the victims' endpoints. Among them are Virtual Network Computing (VNC) and Remote Desktop Protocol (RDP), poorly secured by easy-to-guess username and password combinations; and RATs previously installed in the system.

After fingerprinting the targets—ascertaining if VNC and RDP services exist and are accessible—attackers will attempt to gain access using generic credentials or via brute force. The common denominator in the MajikPOS compromises we've observed involving RATs is the timeline of their infection. The RATs were installed in the endpoints somewhere between August and November, 2016.

If the endpoint piques the malefactors' interest, they use a combination of VNC, RDP, RAT access, command-line FTP (File Transfer Protocol), and sometimes a modified version of Ammyy Admin—a legitimate, commercially available remote administration tool—to install MajikPOS by directly downloading the files usually hosted on free file-hosting sites. In the case of Ammyy Admin, its file manager capability is used instead. The modified version is sometimes named *VNC_Server.exe* or *Remote.exe*.

Configuration and C&C Communication

MajikPOS contacts its C&C server to register the infected system. Once registered, the server then sends a "configuration" with three important entries that will be used in later steps.

Figure 1: C&C server responds with configuration details after registration

The C&C panel in these servers is called "Magic Panel", as shown below:

Figure 2: Magic Panel's login page

RAM-scraping Routine

Conhost.exe is the component responsible for RAM scraping (looking for credit card data on the victim's machine). It uses information from the configuration file for this routine.

MajikPOS checks a sizeable range of cards, such as American Express, Diners Club, Discover, Maestro, Mastercard, and Visa. After verifying the credit card's track data, the information is sent to the C&C server via HTTP POST, Action="bin".

Figure 3: Snapshot of a "Magic Dump" shop selling stolen credit card data

Online Shops for Stolen Credit Card Data

Our foray into one of MajikPOS's C&C servers, umbpan[.]xyz, led us to more websites with the same registrant, one of which is another Magic Panel. The rest of the websites are "Magic Dump" shops where stolen credit card information is sold.

The Dump shops currently contain around 23,400 stolen credit card tracks, sold from US $9 to $39 each, depending on the type of card. They can also be bought in bulk packages of 25, 50, and 100, priced at $250, $400, and $700, respectively. Some of these websites were advertised on carding forums as early as February 2017 by a user called "MagicDumps", who has been updating the forums for new dumps based on location—mostly in the U.S. and Canada.

MajikPOS's Timeline

Here is a rough timeline of events related to MajikPOS, based on our findings:

Other MajikPOS Tricks

MajikPOS was written using .NET. It's an uncommon technique, but not unheard of. GamaPOS, discovered in 2015, was the first documented PoS malware to use the .NET framework. MajikPOS, like many of today's malware, uses encrypted communication to make it harder to detect on the network level. It took advantage of open RDP ports, similar to other related threats like Operation Black Atlas.

We also spotted instances where MajikPOS's operators utilized commonly used lateral movement hacking tools. This can be an indication of their attempts to further access the victim's network. In separate incidents, we saw a command-line tool abused to deploy MajikPOS, along with other PoS malware. MajikPOS is also notable with how it tries to hide by mimicking common file names in Microsoft Windows.

Mitigation

Properly configured chip-and-pin credit cards with end-to-end encryption (EMVs) should be unaffected by this threat. Unfortunately, terminals that don't support them are at risk to threats like MajikPOS.

While the U.S. has adopted EMVs—thanks to the implementation of the EMV Liability Shift last October 2015—the transition has been a challenge. From July 2015 to June 2016, the U.S. lagged behind in terms of EMV-based transactions. While businesses and consumers across the country are increasingly deploying and using chip-based PoS terminals, many merchants, for instance, still haven't implemented the PIN part of the chip-and-PIN process. Although the use of EMV Chip-and-PIN credit cards is not a silver bullet, EMVs are still a

more secure alternative compared to magnetic stripe-based credit cards that are most affected by PoS malware like MajikPOS. In fact, MasterCard and Visa reported a decline in credit card fraud since utilizing EMV-enabled cards and PoS systems.

It would also be useful to take note of a good PoS Defense Model. To further mitigate MajikPOS, it's recommended to properly secure remote access functionalities like remote desktops and VNC, especially when these expose the host or system to the internet. For infosec professionals and IT/system administrators who protect their organization's endpoints, consulting the appropriate documentation for securing Remote Desktop and VNC is a good place to start.

Trend Micro Solutions

Endpoint application control or whitelisting can be employed to reduce attack exposure by ensuring only updates associated with whitelisted applications can be installed. Trend Micro's OfficeScan™ has many security features including Behavior Monitoring, which can be used to detect these names (*csrss.exe* and *conhost.exe*) by the event, "Duplicated System File". It can also detect and prevent other malicious indicators like RATs. Trend Micro's Deep Discovery Inspector can be used to determine attempts to perform lateral movement and possible brute-force activity. MajikPOS's C&C traffic is already blocked by Trend Micro™ Web Reputation Services.

Trend Micro's advanced endpoint solutions such as Trend Micro™ Smart Protection Suites, and Trend Micro™ Worry-Free™ Business Security provide both detection and blocking of all the relevant, malicious files and C&C traffic. Implementing application control in PoS devices also significantly mitigates similar attacks by ensuring that only whitelisted applications are allowed to execute. TippingPoint customers are protected from this threat with the following ThreatDV filter:

27432: HTTP: TSPY_MAJIKPOS.A Checkin

Learn more about our analysis of MajikPOS in this **technical brief**—its Indicators of Compromise (IoCs), an in-depth look into its attack chain and malicious routines, and how the stolen data are sold in underground forums and websites.