LATEST VIDEOS

REVENGE PORN AND SEXTORTION; HOW TO DEAL WITH IT?

HOW DATA BREACH VICTIMS ARE BEING HACKED AGAIN? NEW ATTACK VECTOR

VIEW ALL

POPULAR POSTS:

- How to fake your phone number: Make it look like…
- How to exploit new Facebook feature to access…
- How to Hack Wi-Fi: Cracking WPA2-PSK Passwords Using…
- How to intercept mobile communications (calls and…
- FireEye confirms that APT41 Group hacked TeamViewer;…
- Hack Whatsapp account of your friend
- CREATE YOUR OWN WORDLIST WITH CRUNCH
- List of all Open FTP Servers in the World
- Crack Windows password with john the ripper
- How to scan whole Internet 3.7 billion IP addresses…
- Fake any website in seconds Facebook, Snapchat, Instagram :-
- Do Hacking with Simple Python Script
- Hack Windows, Android, Mac using TheFatRat (Step by…
- How to exploit SUDO via Linux Privilege Escalation
- Hack any website with All in One Tool
- Create your own BotNet (Step By Step tutorial)
- Find Webcams, Databases, Boats in the sea using Shodan
- How to Connect Android to PC/Mac Without WiFi
- Bypass antivirus detection With Phantom Payloads
- Fake text message attack. How Prank or hack your…
- Generate Android App in 2 mins and hack any android mobile
- How to Check if your Mobile phone is hacked or not?
- TOP 6 Hacking mobile Apps – must have
- List of credit cards, proxies on Deep Web
- HIJACKING WHATSAPP ACCOUNTS USING WHATSAPP WEB

VULNERABILITIES

CRITICAL VULNERABILITIES AFFECTING OPENSUSE, FORMERLY SUSE LINUX, DISCLOSED

LILIN IP CAMERAS AND ZYXEL NAS DEVICES HACKED TO LAUNCH DDOS ATTACKS; PROTECT YOUR IOT DEVICES

MEMORY LEAK AND PRIVILEGE ESCALATION VULNERABILITIES IN FREEBSD; MILLIONS OF DEVICES AFFECTED

VIEW ALL

TICK CYBERESPIONAGE GROUP ZEROS IN ON JAPAN

Share this...

Compromised websites and spear-phishing emails used to infect targets with Daserf Trojan. A longstanding cyberespionage campaign has been targeting mainly Japanese organizations with its own custom-developed malware (Backdoor.Daserf). The group, known to Symantec as Tick, has maintained a low profile, appearing to be active for at least 10 years prior to discovery.

In its most recent campaign, Tick employed spear-phishing emails and compromised a number of Japanese websites in order to infect a new wave of victims. The group is highly selective in its approach and only appears to deploy its full range of tools once it establishes that the compromised organization is an intended target. Tick also uses a range of hacktools to map the victim's network and attempt to escalate privileges further.

Daserf's main purpose is information stealing and the Trojan is capable of gathering information from infected computers and relaying it back to attacker-controlled servers. Tick's most recent attacks have concentrated on the technology, aquatic engineering, and broadcasting sectors in Japan.

Recent attacks

Symantec discovered the most recent wave of Tick attacks in July 2015, when the group compromised three different Japanese websites with a Flash (.swf) exploit to mount watering hole attacks. Visitors to these websites were infected with a downloader known as Gofarer (Downloader.Gofarer). Gofarer collects information about the compromised computer and then downloads and installs Daserf.

Tick also used spear-phishing emails in these recent attacks. While Symantec did not find the emails themselves, it did identify the use of an exploit designed to take advantage of a vulnerability in Microsoft Office documents (CVE-2014-4114). This was used to distribute malware in addition to the watering hole activity.

Tick under the microscope

Daserf appears to be custom-developed for use in Tick's cyberespionage campaigns. Once installed, it establishes a remote connection to Tick's command and control server, providing the attacker with access to the compromised computer.

Fig1_35.png

Figure 1. Chain of infection seen in recent Japanese attacks

Once the malware is installed on a targeted computer, the attackers attempt to enumerate the network and escalate their privilege level. To do this, Tick uses a number of publicly available hacktools such as Mimikatz, GSecdump, and Windows Credential Editor. The tools are downloaded and deployed to the original install directory previously created by the malware.

Tick's primary objective appears to be the theft of sensitive information from targeted Japanese organizations. To date, Symantec has observed the group attempting to steal emails and documents such as PowerPoint presentations.

Low-profile threat

The Daserf Trojan employs a number of tactics to avoid detection. Once collected, the stolen data is hidden in password-protected .rar archives.

Daserf also uses file and folder names related to legitimate programs often found in Windows environments in order to blend in. Observed folder names include HP, Intel, Adobe, and perflogs and folders are generally created in either the root drive or the Application Data or Program Files folders. File names used in recent attacks include adobe.exe, adobe_sl.exe, intel.exe, and intellog.exe.

Command and control servers

Tick uses compromised web servers to distribute malware and, in some instances, for its command and control (C&C) infrastructure. However, in most cases, it relies on its own infrastructure for C&C purposes.

In its most recent campaigns, the group registered the domains used for C&C servers days after the malware was compiled. For example, one of the variants of Daserf used was compiled on July 8, 2015. This sample was seen contacting the C&C domain www[.]dreamsig[.]com, which was first registered on July 13, 2015, five days after the compilation date. This pattern occurred in multiple Daserf samples.

Another interesting aspect of the communication between the malware and the C&C infrastructure is how the malware changes the URL from a randomly chosen variable selected from a predefined list.

PREDEFINED LIST FROM DASERF MD5: 765017E16842C9EB6860A7E9F711B0DB
rjdyw.asp
xszgj.asp
dheyf.asp
ejdhf.asp
gxbne.asp
swetf.asp
qgfhr.asp
whjdh.asp
zgfer.asp
cshyr.asp
fxkle.asp
tmwry.asp
viksr.asp
ycghw.asp

Table 1. An example of how a Daserf sample uses a predefined list of URLs embedded in the malware

Symantec identified multiple C&C domains used by Tick. Unfortunately, Tick frequently used either privacy protection services or domain brokers to mask registration information. These tactics are used to make discovery and attribution more difficult.

C&C DOMAIN	PARENT HASH
charlie-harada[.]com	122652ca6ef719f8ba2d8d412ea184fe
isozaki.sakura.ne[.]jp	4601e75267d0dcfe4256c43f45ec470a
www.aucsellers[.]com	7ec173d469c2aa7a3a15acb03214256c
www.lunwe[.]com	8d5bf506e55ab736f4c018d15739e352
c-saika[.]jp	3fa5965a1de2c095de38f22f0645af3e b33f4b8e776b94dc48c234ce9897cf74
kcm-store[.]com	63fe9f06068823b02b925e4a74a57db0
htpc[.]jp	a629926313ee12163e1bdd2bb633e0e2 d3031438d80913f21ec6d3078dc77068
rlsolar[.]jp	d3031438d80913f21ec6d3078dc77068

Table 2. Examples of Tick C&C domains and associated MD5 hashes

Stolen digital certificates used in selected cases

The majority of the malware analyzed was not digitally signed. However, a small percentage was signed with a stolen digital certificate. It is unclear why the certificate was used so sparingly, since signed malware would receive a greater level of trust and reduce the risk of detection.

It is possible that the certificate was used against a target that had a secure environment which may have required binaries to be signed in order to interact with the operating system.

The issuer of the certificate has been informed of its misuse and confirmed that it would be revoked.

Fig2_24.png

Figure 2. The stolen digital certificate used to sign Tick malware

Targets

The use of compromised websites to infect victims results in unintentional infections, making it difficult to identify the motives of the attacker. By searching for evidence of post-infection activity, Symantec identified seven organizations where Tick had mounted persistent post-compromise attacks. These organizations were primarily large Japanese technology, engineering, and media firms.

Fig3_20.png

Figure 3. Daserf infections by region

The seven organizations therefore appear to be Tick's intended targets. In addition to seeing post-compromise tools used in these attacks, the length of time the attackers were active on the networks provided additional evidence that these were high-value targets. The longest time Tick was active in a victim's environment was 18 months. The average timeframe was five months and the number of infected hosts in a victim's network ranged from 3 to 15 systems.

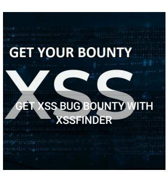
Conclusion

Tick has left a trail of evidence indicating that its activity began as early as 2006. In earlier attacks, the group used malicious Microsoft Word documents to infect victims, with compromised websites being added to the mix as a more recent attack vector.

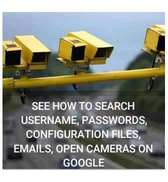
Tick appears to be a well-organized group, with the funding and capability to develop and update its malware. It has the ability to compromise legitimate infrastructure to use for malware distribution and has access to stolen digital certificates to sign its malware when needed. Tick primarily uses purchased infrastructure for its C&C servers and has been able to stay off the radar since 2006.

Tick exhibits all the hallmarks of an advanced cyberespionage group. The long lifespan of the group, as well as the consistent targeted attacks against specific industries, support this theory. The individuals or organization behind Tick's operations has an interest in Japanese technology along with Japanese media and broadcasting organizations. While Tick's tactics may change over time, the group's history indicates that its focus will continue to be a narrow range of targets, mainly in Japan.

Source:https://www.symantec.com/



GET XSS BUG BOUNTY WITH XSSFINDER


SEE HOW TO SEARCH USERNAME, PASSWORDS, CONFIGURATION FILES, EMAILS, OPEN CAMERAS ON GOOGLE

NEW LINUX FOR CYBER FORENSICS AND INVESTIGATORS – CSI LINUX

Alisa Esage

Working as a cyber security solutions architect, Alisa focuses on bug bounty and network security. Before joining us she held a cyber security researcher positions within a variety of cyber security start-ups. She also experience in different industry domains like finance, healthcare and consumer products.

Share this...

ON: APRIL 30, 2016 / IN: DATA SECURITY, MALWARE, VULNERABILITIES / TAGGED: JAPAN., TROJAN

TUTORIALS

MEET SWISS ARMY KNIFE OF PENETRATION TESTING

NEW PENETRATION TESTING FRAMEWORK FOR HACKERS

REDRABBIT FOR #REDTEAM TO CONDUCT ETHICAL HACKING

RUN PROGRAM WITHOUT ADMINISTRATOR PRIVILEGES IN WINDOWS

HOW TO USE FACEBOOK FOR OPEN SOURCE INVESTIGATION (OSINT)

GET XSS BUG BOUNTY WITH XSSFINDER

SEE HOW TO SEARCH USERNAME, PASSWORDS, CONFIGURATION FILES, EMAILS, OPEN CAMERAS ON GOOGLE

NEW LINUX FOR CYBER FORENSICS AND INVESTIGATORS – CSI LINUX

SCAN WHOLE INTERNET DOMAINS, WITH SPEED OF 3,50,000 DOMAINS PER SECOND

ATTACK ANY IP ADDRESS, WITH DDOS BOTNET SIMULATOR

VIEW ALL

MALWARE

COVID-19 TRACKING APP INSTALLS RANSOMWARE ON YOUR SMARTPHONE; BE CAREFUL

NEW MALWARE PROMISES NUDE PHOTOS OF YOUR GIRLFRIEND OR FRIEND'S GIRLFRIEND

THESE MEDICAL DEVICES COULD BE EASILY ENCRYPTED WITH WANNACRY RANSOMWARE

EASILY REMOVE XHELPER MALWARE FROM YOUR ANDROID DEVICE

NEW RANSOMWARE DEMANDS PHOTOS OF TITS & PRIVATE PARTS TO UNLOCK YOUR DATA

VIEW ALL

CYBER SECURITY CHANNEL

THE MOST DANGEROUS & SPYING TELEVISION AWARD GOES TO TCL

US STATE SEATTLE WILL ALLOW ONLINE VOTING BY SMARTPHONE IN 2020 ELECTIONS

CYBER THREATS & FUTURE OF CYBER SECURITY: RAJ SAMANI MCAFEE CHIEF SCIENTIST