Related news

cyberscoop.com/nsa-shadow-brokers-leaks-iran-russia-optimusprime-stoicsurgeon/

April 18, 2017

government

Shadow Brokers leaks show U.S. spies successfully hacked Russian, Iranian targets

(Creative Time Reports / Flickr)
Written by Chris Bing
Apr 18, 2017 | CYBERSCOOP
The leaked NSA documents and tools published in recent months by the mysterious Shadow Brokers group have provided rare insight into the clandestine digital espionage operations pursued by the spy agency over the past few years, including information on operations aimed at Iran and Russia.

Last Friday the rogue group released a new package of NSA files, this time detailing numerous tools designed to break into older versions of Microsoft Windows and a campaign to compromise banking networks in the Middle East. Additional targets were also mentioned

one week prior in a separate archive that was largely ignored by most media outlets.

Yet the document cache published April 8 provides evidence that the NSA had once launched a series of successful computer-based intrusions against multiple high-profile foreign targets, including the Office of the President of Iran and the Russian Federal Nuclear Center, said two former intelligence officials who spoke to CyberScoop on the condition of anonymity due to their knowledge of internal operations. That release contained files with earmarked organizations and other evidence that explains how certain cyberattacks were engineered.

“The fact that this is in there the way it is means these targets were definitely owned,” one former intelligence official said. “It means it was a successful op, plain and simple.”

Another former intelligence official that worked at the NSA and also spoke on condition of anonymity said the April 8 document dump offered authentic internal information regarding past agency operations.

While the Shadow Brokers published a list of 300 IP addresses last October that were supposedly once compromised by the spy agency, it was not until recently that researchers were provided with more comprehensive targeting data.

An analysis of one archive presented by the Shadow Brokers reveals a collage of web domains and hardware systems that were at one point targeted by the NSA and attacked with a suite of hacking tools. These domains include:

- dolat.ir: Islamic Republic of Iran Presidential Office website
- vniitf.ru: Russian Federal Nuclear Center website
- mail.prf.gov.ru: a mail server for the Presidential Administration of Russia (aprf.gov.ru is no longer online)
- vega-int.ru: a website for Russian internet service provider, Vega-Internet
- snz.ru: a website for the office providing telecommunications and other internet support for Vniitf.ru
- minatom.ru: a website of the Ministry for Atomic Energy of the Russian Federation
- udprf.ru: the Office of the President of the Russian Federation website
- rowdaco.com: a defunct website once apparently used by a Somalia-based electronics store, Rowda Electronics Company
- ikoula.com: a website for a French data storage and server rental company

A closer look at the full filenames in the archive provides additional insight. The websites themselves represent targeted host machines, or boxes, each of which is paired with two different codenames— one for the hacking tool used and another for the associated operation.

For example, one such file name is listed as:

> *stoicsurgeon_ctrl__v__1.5.33.2_x86-linux-optimusprime-vezarat.dolat.ir*

In this context, the term “stoicsurgeon” is a reference to the codename of the deployed tool. “Optimusprime” is the title of an NSA operation. “v__1.5.33.2” details the version of stoicsurgeon, a rootkit backdoor aimed at Linux’s MultiArch — which helps install library packages from multiple architectures on the same machine.

Experts say stoicsurgeon is a post-exploitation tool, meaning that a different exploit was necessary to first compromise the target. “Ctrl” in the sample is the name of the loader. “x86-Linux” refers to the 32-bit Linux operating system used by the target in this case. “Vezarat,” a term referring to Iran’s Ministry of Intelligence, is the host box in the dolat.ir domain that was specifically compromised.

It all translates to an NSA operation that likely saw U.S. spies hack into a host box inside a computer network that was of high interest to national security analysts in Washington during the Obama administration. According to an internal PowerPoint presentation previously leaked by former agency contractor Edward Snowden, “Optimusprime” is related to the NSA’s SPINALTAP project, a program that was introduced to combine data from active operations and passive signals intelligence.

Stoicsurgeon is just one hacking tool used against the web domains listed above. Another tool, codenamed “suctionchar,” also features prominently in the archive filename list — for example: *suctionchar_agent__v__2.0.27.18_x86-linux-tilttop-comet.vniitf.ru*.

Security researcher x0rz described “suctionchar” as a “32 or 64 bit OS, solaris sparc 8,9, Kernel level implant” that provide an attacker with “transparent, sustained, or realtime interception of processes input/output vnode traffic,” that can also “intercept ssh, telnet, rlogin, rsh, password, login, [and] csh” data.