Regin (malware)

By Contributors to Wikimedia projects

Published: 2014-11-23 · Archived: 2026-04-05 13:44:28 UTC

From Wikipedia, the free encyclopedia

Regin	
Malware details	
Aliases	Prax, QWERTY
Authors	NSA, GCHQ
Technical details	
Platform	Windows

Regin (also known as **Prax** or **QWERTY**) is a sophisticated malware and hacking toolkit used by United States' National Security Agency (NSA) and its British counterpart, the Government Communications Headquarters (GCHQ).[1][2][3] It was first publicly revealed by Kaspersky Lab, Symantec, and The Intercept in November 2014.[4][5] The malware targets specific users of Microsoft Windows-based computers and has been linked to the US intelligence-gathering agency NSA and its British counterpart, the GCHQ.[6][7][8] *The Intercept* provided samples of Regin for download, including malware discovered at a Belgian telecommunications provider, Belgacom.[5] Kaspersky Lab says it first became aware of Regin in spring 2012, but some of the earliest samples date from 2003.[9] (The name Regin is first found on the VirusTotal website on 9 March 2011.[5]) Among computers infected worldwide by Regin, 28 percent were in Russia, 24 percent in Saudi Arabia, 9 percent each in Mexico and Ireland, and 5 percent in each of India, Afghanistan, Iran, Belgium, Austria, and Pakistan.[10]

Kaspersky has said the malware's main victims are private individuals, small businesses and telecom companies. Regin has been compared to Stuxnet and is thought to have been developed by "well-resourced teams of developers", possibly a Western government, as a targeted multi-purpose data collection tool.[11][12][13]

According to *Die Welt*, security experts at Microsoft gave it the name "Regin" in 2011, after the cunning Norse dwarf Regin.[14]

Regin uses a modular approach allowing it to load features that exactly fit the target, enabling customized spying. The design makes it highly suited for persistent, long-term mass surveillance operations against targets.[15][16]

Regin is stealthy and does not store multiple files on the infected system; instead it uses its own encrypted virtual file system (EVFS) entirely contained within what looks like a single file with an innocuous name to the host, within which files are identified only by a numeric code, not a name. The EVFS employs a variant encryption of

the rarely used RC5 cipher.[16] Regin communicates over the Internet using ICMP/ping, commands embedded in HTTP cookies and custom TCP and UDP protocols with a command and control server which can control operations, upload additional payloads, etc.[10][12]

Identification and naming

[edit]

Symantec says that both it and Kaspersky identified the malware as *Backdoor.Regin*.[10] Most antivirus programs, including Kaspersky, (as of October 2015) do NOT identify the sample of Regin released by The Intercept as malware.[17] On 9 March 2011 Microsoft added related entries to its Malware Encyclopedia;[18][19] later two more variants, *Regin.B* and *Regin.C* were added. Microsoft appears to call the 64-bit variants of Regin *Prax.A* and *Prax.B*. The Microsoft entries do not have any technical information.[5] Both Kaspersky and Symantec have published white papers with information they learned about the malware.[12][13]

Known attacks and originator of malware

[edit]

German news magazine *Der Spiegel* reported in June 2013 that the US intelligence National Security Agency (NSA) had conducted online surveillance on both European Union (EU) citizens and EU institutions. The information derives from secret documents obtained by former NSA worker Edward Snowden. Both *Der Spiegel* and *The Intercept* quote a secret 2010 NSA document stating that it made cyberattacks that year, without specifying the malware used, against the EU diplomatic representations in Washington, D.C. and its representations to the United Nations.[5][20] Signs identifying the software used as Regin were found by investigators on infected machines.

The Intercept reported that, in 2013, the UK's GCHQ attacked Belgacom, Belgium's largest telecommunications company.[5] These attacks may have led to Regin coming to the attention of security companies. Based on analysis done by IT security firm Fox IT, *Der Spiegel* reported in November 2014, that Regin is a tool of the UK and USA intelligence agencies. Fox IT found Regin on the computers of one of its customers, and according to their analysis parts of Regin are mentioned in the NSA ANT catalog under the names "Straitbizarre" and "Unitedrake". Fox IT did not name the customer, but *Der Spiegel* mentioned that among the customers of Fox IT is Belgacom and cited the head of Fox IT, Ronald Prins, who stated that they are not allowed to speak about what they found in the Belgacom network.[1]

In December 2014, German newspaper *Bild* reported that Regin was found on a USB flash drive used by a staff member of Chancellor Angela Merkel. Checks of all high-security laptops in the German Chancellery revealed no additional infections.[21]

Regin was used in October and November 2018 to hack the research and development unit of Yandex.[22]

- Advanced persistent threat
- Cyberwarfare in the United States

- NSA ANT catalog
- Stuxnet
- WARRIOR PRIDE

1. ^ Jump up to: a b Christian Stöcker, Marcel Rosenbach " Spionage-Software: Super-Trojaner Regin ist eine NSA-Geheimwaffe" Der Spiegel, November 25, 2014
2. ^ *"Experts Unmask 'Regin' Trojan as NSA Tool"*. *Spiegel.de. Retrieved 9 November 2021.*
3. ^ *Zetter, Kim. "Researchers Uncover Government Spy Tool Used to Hack Telecoms and Belgian Cryptographer". Wired. ISSN 1059-1028. Retrieved 2022-02-22.*
4. ^ *"Regin Revealed". Kaspersky Lab. 24 November 2014. Retrieved 24 November 2014.*
5. ^ Jump up to: a b c d e f *Marquis-Boire, Morgan; Guarnieri, Claudio; Gallagher, Ryan (24 November 2014). "Secret Malware in European Union Attack Linked to U.S. and British Intelligence". The Intercept. The Intercept. Archived from the original on 29 July 2015. Retrieved 24 November 2014.*
6. ^ *"Top German official infected by highly advanced spy trojan with NSA ties". 26 October 2015.*
7. ^ *Perlroth, Nicole (24 November 2014). "Symantec Discovers 'Regin' Spy Code Lurking on Computer Networks". New York Times. Retrieved 25 November 2014.*
8. ^ *Gallagher, Ryan (13 December 2014). "The Inside Story of How British Spies Hacked Belgium's Largest Telco". The Intercept. Archived from the original on 17 August 2015. Retrieved 13 June 2015.*
9. ^ Kaspersky:Regin: a malicious platform capable of spying on GSM networks, 24 November 2014
10. ^ Jump up to: a b c *"Regin: Top-tier espionage tool enables stealthy surveillance". Symantec. 23 November 2014. Retrieved 25 November 2014.*
11. ^ *"BBC News - Regin, new computer spying bug, discovered by Symantec". BBC News. 23 November 2014. Retrieved 23 November 2014.*
12. ^ Jump up to: a b c *"Regin White Paper" (PDF). Symantec. Archived from the original (PDF) on 7 September 2019. Retrieved 23 November 2014.*
13. ^ Jump up to: a b *"Regin White Paper" (PDF). Kaspersky Lab. Retrieved 24 November 2014.*
14. ^ *Benedikt Fuest (24 November 2014). "Ein Computervirus, so mächtig wie keines zuvor". Die Welt. Archived from the original on 28 November 2014.*
15. ^ *"Regin Malware - 'State-Sponsored' Spying Tool Targeted Govts". The Hacking Post - Latest hacking News & Security Updates. Archived from the original on 2017-02-18. Retrieved 2014-11-24.*
16. ^ Jump up to: a b *"NSA, GCHQ or both behind Stuxnet-like Regin malware?". SC Magazine UK. scmagazineuk.com. 24 November 2014. Archived from the original on 16 June 2016. Retrieved 25 November 2014.*
17. ^ Virustotal: Detection ratio: 21 / 56
18. ^ Microsoft Malware Protection Center, click button "Malware Encyclopedia
19. ^ Microsoft Protection Center: Trojan:WinNT/Regin.A
20. ^ *Poitras, Laura; Rosenbach, Marcel; Schmid, Fidelius; Stark, Holger (29 June 2013). "Attacks from America: NSA Spied on European Union Offices". Der Spiegel.*
21. ^ *"German government denies falling victim to cyber attack". Deutsche Welle. 29 December 2014.*
22. ^ *"Western Intelligence Hacked 'Russia's Google' Yandex to Spy on Accounts". Reuters. June 27, 2019. Archived from the original on June 29, 2019.*