PLATINUM (cybercrime group)

By Contributors to Wikimedia projects

Published: 2017-06-09 · Archived: 2026-04-05 20:01:27 UTC

From Wikipedia, the free encyclopedia

PLATINUM is the name given by Microsoft to a cybercrime collective active against governments and related organizations in South and Southeast Asia.[1] They are secretive and not much is known about the members of the group.[2] The group's skill level is such that its attacks sometimes go without detection for many years.[1]

The group, considered an advanced persistent threat, has been active since at least 2009,[3] targeting victims via spear-phishing attacks against government officials' private email addresses, zero-day exploits, and hot-patching vulnerabilities.[4][5] Upon gaining access to their victims' computers, the group steals economically sensitive information.[1]

PLATINUM succeeded in keeping a low profile until their abuse of the Microsoft Windows hot patching system was detected and publicly reported in April 2016.[2] This hot patching method allows them to use Microsoft's own features to quickly patch, alter files or update an application, without rebooting the system altogether. This way, they can maintain the data they have stolen while masking their identity.[2]

In June 2017, PLATINUM became notable for exploiting the serial over LAN (SOL) capabilities of Intel's Active Management Technology to perform data exfiltration.[6][7][8][9][10][11][12][13]

PLATINUM's techniques

[edit]

PLATINUM has been known to exploit web plugins, at one point infiltrating the computers of several Indian government officials 2009, using a website that provided an email service.[1]

Once in control of a target's computer, PLATINUM actors can move through the target's network using specially built malware modules. These have either been written by one of the multiple teams working under the Platinum group umbrella, or they could have been sold through any number of outside sources that Platinum has been dealing with since 2009.[1]

Because of the diversity of this malware, the versions of which have little code in common, Microsoft's investigators have taxonomised it into families.[1]

The piece of malware most widely used by PLATINUM was nicknamed Dispind by Microsoft.[1] This piece of malware can install a keylogger, a piece of software that records (and may also be able to inject) keystrokes. [*citation needed*]

PLATINUM also uses other malware like "JPIN" which installs itself into the %appdata% folder of a computer so that it can obtain information, load a keylogger, download files and updates, and perform other tasks like extracting files that could contain sensitive information.[1]

"Adbupd" is another malware program utilised by PLATINUM, and is similar to the two previously mentioned. It is known for its ability to support plugins, so it can be specialised, making it versatile enough to adapt to various protection mechanisms.[1]

In 2017, Microsoft reported that PLATINUM had begun to exploit a feature of Intel CPUs.[14] The feature in question is Intel's AMT Serial-over-LAN (SOL), which allows a user to remotely control another computer, bypassing the host operating system of the target, including firewalls and monitoring tools within the host operating system.[14]

Microsoft advises users to apply all of their security updates to minimize vulnerabilities and to keep highly sensitive data out of large networks.[1] Because PLATINUM targets organizations, companies and government branches to acquire trade secrets, anyone working in or with such organizations can be a target for the group.[15]

- Intel AMT § Known vulnerabilities and exploits
- Titanium (malware)

1. ^ Jump up to: *a b c d e f g h i j* *"PLATINUM Targeted attacks in South and Southeast Asia (PDF)"* *(PDF). Windows Defender Advanced Threat Hunting Team (Microsoft). 2016. Retrieved 2017-06-10.*
2. ^ Jump up to: *a b c* *Osborne, Charlie. "Platinum hacking group abuses Windows patching system in active campaigns". ZDNet. Retrieved 2017-06-09.*
3. ^ *Eduard Kovacs (2017-06-08). ""Platinum" Cyberspies Abuse Intel AMT to Evade Detection". SecurityWeek.Com. Retrieved 2017-06-10.*
4. ^ *Eduard Kovacs (2016-04-27). ""Platinum" Cyberspies Abuse Hotpatching in Asia Attacks". SecurityWeek.Com. Retrieved 2017-06-10.*
5. ^ *msft-mmpc (2016-04-26). "Digging deep for PLATINUM – Windows Security". Blogs.technet.microsoft.com. Retrieved 2017-06-10.*
6. ^ *Peter Bright (2017-06-09). "Sneaky hackers use Intel management tools to bypass Windows firewall". Ars Technica. Retrieved 2017-06-10.*
7. ^ *Tung, Liam (2014-07-22). "Windows firewall dodged by 'hot-patching' spies using Intel AMT, says Microsoft". ZDNet. Retrieved 2017-06-10.*
8. ^ *msft-mmpc (2017-06-07). "PLATINUM continues to evolve, find ways to maintain invisibility – Windows Security". Blogs.technet.microsoft.com. Retrieved 2017-06-10.*
9. ^ *Catalin Cimpanu (2017-06-08). "Malware Uses Obscure Intel CPU Feature to Steal Data and Avoid Firewalls". Bleepingcomputer.com. Retrieved 2017-06-10.*
10. ^ *Juha Saarinen (2017-06-08). "Hackers abuse low-level management feature for invisible backdoor - Security". iTnews. Retrieved 2017-06-10.*
11. ^ *Richard Chirgwin (2017-06-08). "Vxers exploit Intel's Active Management for malware-over-LAN. Platinum attack spotted in Asia, needs admin credentials". The Register. Retrieved 2017-06-10.*

12. ^ *Christof Windeck (2017-06-09). "Intel-Fernwartung AMT bei Angriffen auf PCs genutzt | heise Security". Heise.de. Retrieved 2017-06-10.*
13. ^ *"PLATINUM activity group file-transfer method using Intel AMT SOL | Windows Security Blog | Channel 9". Channel9.msdn.com. 2017-06-07. Retrieved 2017-06-10.*
14. ^ Jump up to: *a b* "Platinum hacker group uses Intel AMT", *Tad Group*, 2017-09-25
15. ^ *Liu, Jianhong (2017-07-15). Comparative Criminology in Asia. Springer. ISBN 9783319549422.*
