New Trojan shows return of script kiddies

The interesting thing about the PRG Trojan is its ability to change so rapidly

Michael Crawford (Computerworld) | **29 June, 2007 13:24** | Comments | Like

Local security firms have confirmed the presence of an online Trojan construction kit designed solely to update variants of itself and grab sensitive passwords and user details from infected users.

The Trojan, dubbed the PRG Trojan by SecureWorks (US) as well as Internet Security Systems (ISS) Australia, is a variant of another Trojan dubbed wnspoem by SecureWorks which was discovered October 2006.

> "It is really taking the tricks learnt in the past and applying them to modern day motives"
>
> Adam Biviano - premium services manager, Trend Micro

The Trojan is designed to search data from the Windows internal memory buffer before the data is encrypted and sent to secure Web sites.

Don Jackson, security researcher at US SecureWorks said already variants of the PRG Trojan have stolen sensitive information from around 10,000 US citizens and sent the information to rogue servers in China, Russia and the US.

According to Jackson the Trojan can be recompiled in countless different ways to evade signature-based detection.

Adam Biviano, Trend Micro Australia premium services manager said the Trojan is a rehash of the script kiddie approach to authoring and sharing malware code and believes this kind of virus development is the future of viruses.

"This Trojan (PRG) is a very good example of a man-in-the-middle attack as it is designed to intercepts requests to encrypted web sites and SSL encryption offers no protection for machine as in SSL transactions the encryption occurs between the machines transporting data but not the end node," Biviano said.

"Wnspoem and the PRG Trojan were all based on this construction kit which enables people to define the properties of the Trojan, how it infects and even what it does."

"It is really taking the tricks learnt in the past and applying them to modern day motives". According to ISS, the construction kit is readily available online and is designed for rapid deployment of new Trojan variants using a variety of different packaging schemas.

"The PRG Trojan itself seems to have the ability to sort through files, sniff data out of HTTP/HTTPS headers (logins, etc) as opposed to actually keylogging, so it can detect "virtual keyboard" inputs, pasted text etc," an ISS spokesperson said.

"Some of the newer variants do appear to listen in on port 6081, but as an additional vector for commands after initial infection. The newer versions can also upload the data via chains of proxies in order to hide the traffic.

"The Trojan can update itself, and the updates can change the data upload sites to further avoid efforts to thwart the data theft (for instance, blocking known sites at the network firewall, etc)."

Declan Ingram, senior security consultant with Australian based information security and advisory company security-assessment.com said the hallmark of both the construction kit and subsequent variants is the dedication and organization of the developers.

Ingram said the developers of the Trojan are "so on top of" efforts to beat signature-based antivirus and security tools.

"The interesting thing about the PRG Trojan is its ability to change so rapidly," Ingram said.

"Due to the dedication and organization of the developers and technical or specific tools to stop it are thwarted in a very short period of time as the code always seems to untie them.

"It has actually been releasing new versions of itself as soon as the current ones are detected by AV companies as there is always a certain amount of time for AV companies to release a patch and end users to put the patch in place — at best 24 hours which is more than enough time for a small change or to have the software do it automatically."

Ingram suggested an organization can block port 6081activity by using strict firewall rules as well as ingress and egress filtering.

"RS you ruined my Nemisis thing, I had that one lined up. ..." on **Report bombs Aussie broadband**

"Michael, if you look at the actual figures you will see that ..." on **AFACT v iiNet: Second chance termination strains resources**

"Hold on a moment. how can we be expected to playpen users ..." on **AFACT: Shape, prevent or playpen, but iiNet did nothing**

Bookmark this page

Share this article

Got more on this story? Email Computerworld