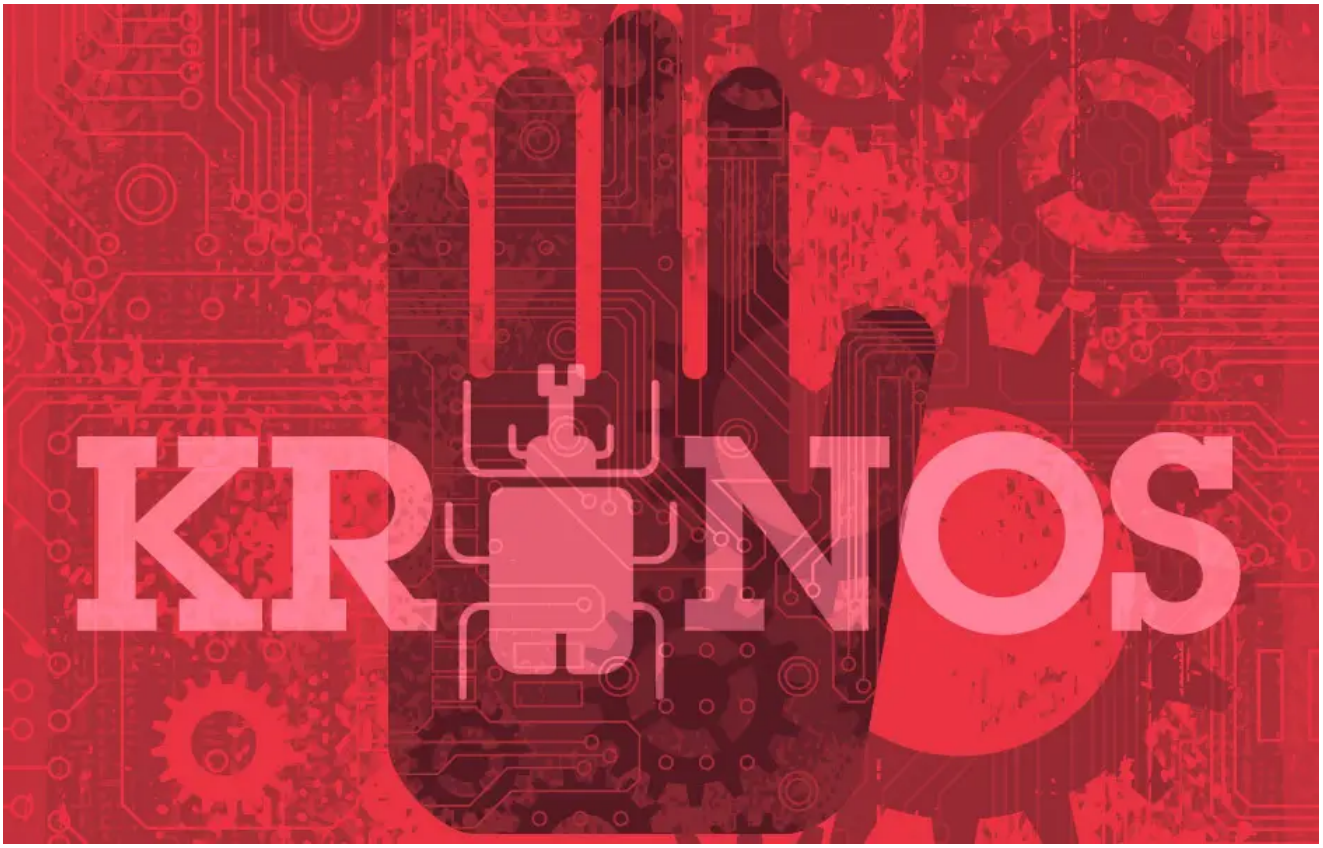
The Father of Zeus: Kronos Malware Discovered

securityintelligence.com/the-father-of-zeus-kronos-malware-discovered/

July 11, 2014



Banking & Finance July 11, 2014

By Etay Maor 3 min read

New Trojan from the Russian Underground

While major players like Zeus, Gozi, Citadel and other advanced financial malware dominate the malware threat landscape, newcomers and challengers always try to get a share of the cyber crime market. One such new malware that was recently made available for purchase in a Russian underground forum is the Kronos malware. With a $7,000 price tag, this malware offers multiple modules for evading detection and analysis as well as an option to test the malware for a week prior to buying it.

Note that the following descriptions of Kronos are based solely on entries in the underground forum; Trusteer, an IBM company, has not yet analyzed a malware sample in order to validate the seller's claims.

Kronos Malware: Like Father, Like Son?

We recently found a cyber criminal offering the Kronos malware to members of a major Russian underground forum. The forum post details several of the malware's technical capabilities and concludes with information on business and purchase options. From the malware's description, several elements are worth noting:

- Common credential-stealing techniques such as form grabbing and HTML injection compatible with the major browsers (Internet Explorer, Firefox and Chrome);
- 32- and 64-bit ring3 (user-mode) rootkit capable of also "defending from other Trojans";
- Antivirus bypassing;
- Malware-to-C&C communication encryption;
- Sandbox bypassing.

Consistent with other financial malware developments, it seems that significant time and effort were given to evading security tools used both by end users and security white hats. In addition, the HTML injection mechanism is compatible with Zeus. Because Zeus is the most widely deployed malware, and it is likely that potential clients have used or still use Zeus variants, the authors of Kronos made sure that the HTML injection files used by Zeus operators can be easily implemented with Kronos. Coincidence or not, it is also worth noting that in Greek mythology, Kronos is Zeus' father.

The business side of this offer is interesting as well. Most malware today is sold in the low hundreds of dollars, sometimes even offered for free due to several malware source code leaks. Comparatively, the Kronos malware carries a hefty cost of $7,000. This price, however, is not the first time a new malware seller has demanded a premium. Approximately four years ago, Carberp was released and priced at $10,000 (and $15,000 for the addition of the VNC module, which is almost a standard capability of today's financial malware). The Kronos seller also offers a one-week testing server for $1,000, during which time a potential client will have access to the malware's control panel and all the bot's capabilities.

The authors promise to develop new modules for the malware (which will be charged separately), along with updates and bug fixes (free of charge). The preferred payment methods for this deal are various forms of e-currency such as Perfect Money and Bitcoin. As an incentive, early buyers are promised a discounted price.

It remains to be seen how popular Kronos will be within the cybercrime community. Trusteer's security team continues to monitor underground forums for new threats as well as analyze, reverse engineer and study new malware files.

I present you a new banking Trojan

Compatible with 64 and 32bit rootkit Trojan is equipped with the tools to give you successful banking actions.Formgrabber: Works on Chrome, IE, FF in latest versions. Works on the majority of older versions as well. Steals logs from each website Webinjects: Works on latest Chrome, IE, FF, latest and majority of older versions. Injections are in Zeus config format, so it's easy to transfer the config from one another.32 and 64bit Ring3 rootkit: The Trojan also has a ring 3 rootkit that defends it from other Trojans.

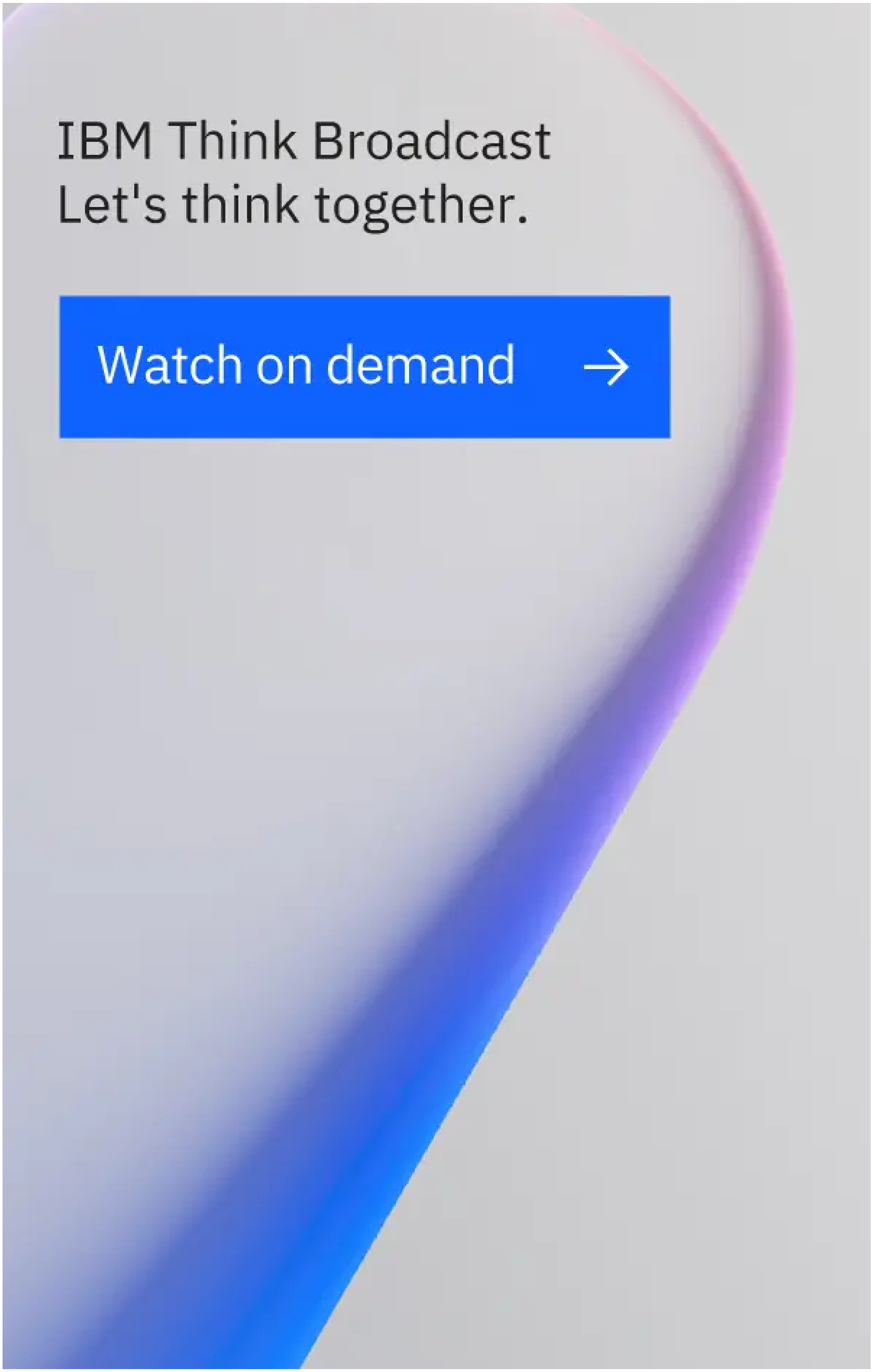
Proactive Bypass: The Trojan uses an undetected injection method to work in a secure process and bypass proactive anti-virus protections. Encrypted Communication: Connection between bot and panel is encrypted to protect against sniffers. Usermode Sandbox and rootkit bypass: The Trojan is able to bypass any hook in usermode functions which bypasses rootkits or sandboxes which use these hooks.

1000$ a week of testing. The server will be hosted only for you. You need just a domain or a payment including the domain fee. You'll have full access to the C&C, without any limits or restrictions during test mode.7000$ Lifetime product license, free updates and bug removals. New modules will not be free , and you will need to pay additionally. We accept Perfect Money, Bitcoin, WMZ, BTC-E.comCurrently the Trojan is written in its fullest. Next week we will have tests and bug fixing, then release. Pre-ordering the Trojan will give you a discount.

Etay Maor
Executive Security Advisor, IBM Security

Etay Maor is an Executive Security Advisor at IBM Security, where he leads security and fraud fighting awareness and research. A security evangelist, Etay re...

think2022 IBM



IBM Think Broadcast
Let's think together.

Watch on demand →