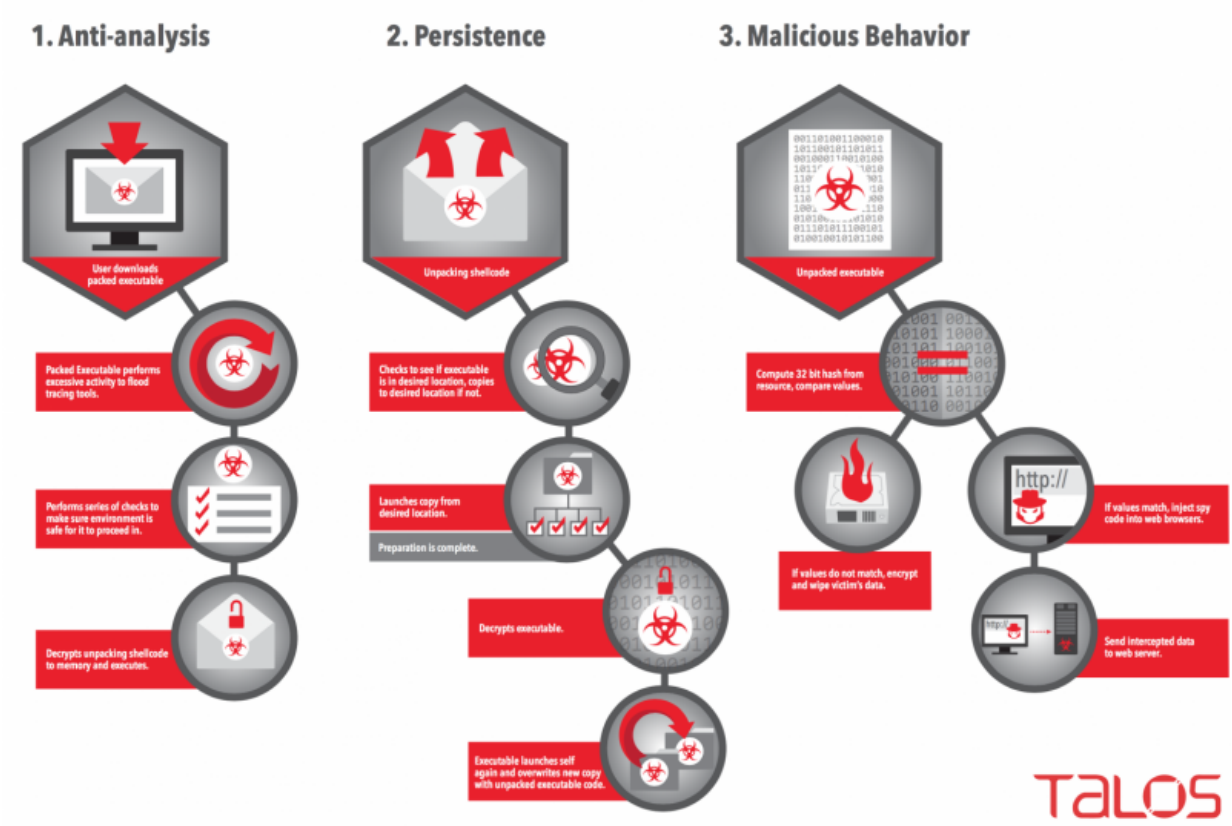
Rombertik malware: evasive, layered, out to steal

May 6 2015, by Nancy Owano



An illustration of the step-by-step process Rombertik follows to compromise the target system. Credit: Talos Group

By now, you can at least compose some of the story line for a made-for-Hollywood script. Ten times over. Researchers at XYZ discover malware

that steals login credentials and data. The malware du jour is given a menacing name; relevant spokespeople say they are working on a patch. Victims receive advice, such as Be Careful.

Now here's a real twist. This one is called Rombertik. BBC News said Tuesday that Rombertik gets especially nasty if it detects that someone is trying to understand how it works. In that case, Rombertik renders the PC useless; deleting key files and making the machine constantly restart.

Ben Baker, research engineer and Alex Chiu, threat researcher, both from the Talos Security Intelligence and Research Group at Cisco, provided a detailed look at the malware sample Rombertik, which they identified—reverse-engineering it and realizing there were a number of layers to it "of obfuscation and anti-analysis functionality."

Debugging is no walk in the park; Rombertik was designed to evade static and dynamic analysis tools. The two researchers said that if the sample picked up on the fact it was being analyzed or debugged, it would destroy the master boot record (MBR).

Jeremy Kirk, Australia Correspondent, IDG News Service, did not try to mince his words when he called the malware terrifying and reported that it resorts to crippling a computer if detected during security checks.

"Rombertik goes through several checks once it is up and running on a Windows computer to see if it has been detected," he wrote Tuesday."The last check Rombertik does is the most dangerous one. It computes a 32-bit hash of a resource in memory, and if either that resource or the compile time had been changed, Rombertik triggers self-destruct."

Michael Mimoso of *Threatpost,* the security news service of Kaspersky Lab, delivered a discussion of Rombertik, which he said had been

discovered earlier in the year and dubbed Rombertik by researchers at Cisco Talos.

In their Cisco blog, Baker and Chiu wrote that "If Rombertik detects an instance of Firefox, Chrome, or Internet Explorer, it will inject itself into the process and hook API functions that handle plain text data. Once accomplished, Rombertik is then able to read any plain-text data the user might type into their browser and capture this input before it gets encrypted if the input is to be sent over HTTPS. This enables the malware to collect data such as usernames and passwords from almost any website. Rombertik does not target any site in particular, such as banking sites, but instead, attempts to steal sensitive information from as many websites as possible."

The BBC said that analysts found the data-stealing attacker unique among malware samples for resisting capture so aggressively.

The attackers use social engineering tactics to entice users to download, unzip, and open attachments. A case in point is an organization making a business pitch to work with an enterprise, inviting the potential victim to check out an attachment to see if the two businesses are aligned for a successful relationship.

Baker and Chiu discussed a sample message in Rombertik's distribution that appeared to come from the "Windows Corporation," with "state-of-the-art manufacturing quality processes." The attackers try to convince the user to check document attachments "to see if their business aligns with the target user's organization. If the user downloads and unzips the file, the user then sees a file that looks like a document thumbnail."

The file may appear to be some sort of PDF from the icon or thumbnail, said the researchers, but the file is a .SCR screensaver executable file containing Rombertik. "Once the user double clicks to open the file,

Rombertik will begin the process of compromising the system."

More information: blogs.cisco.com/security/talos/rombertik