Tinba Malware Reloaded and Attacking Banks Around the World

securityintelligence.com/tinba-malware-reloaded-and-attacking-banks-around-the-world/

September 22, 2014

Home / Banking & Finance

Tinba Malware Reloaded and Attacking Banks Around the World

Banking & Finance September 22, 2014
By Assaf Regev co-authored by Tal Darsan 5 min read
Julia Karpin contributed research for this blog.

IBM Security Trusteer researchers, in addition to those from Avast, recently identified a new variant of the Tinba malware, which had its source code leaked in July. The variant is exhibiting some interesting new features, including techniques to bypass automated security controls and the ability to "phone home," even if the original command-and-control (C&C) center has been taken down.

Initially, only a handful of financial institutions were targeted. However, at the time of this posting, this attack had broadened to include a larger number of banks globally — including the United States and Canada. Our research teams have been tracking and flagging these files as malicious with a combination of low (2/55) and high (22/53) detection rates in VirusTotal (VT) in addition to samples that have yet to be submitted to VT.

According to an analysis conducted by IBM Trusteer researchers, the malware seems to have been assembled from the leaked source code of the well-known Tinba malware, one of the most sophisticated financial malware toolkits available today. Since the leak of Tinba's source code in July, new functionality has appeared, improving malware stealth, recovery mechanisms against takedown attempts and new behavioral changes.

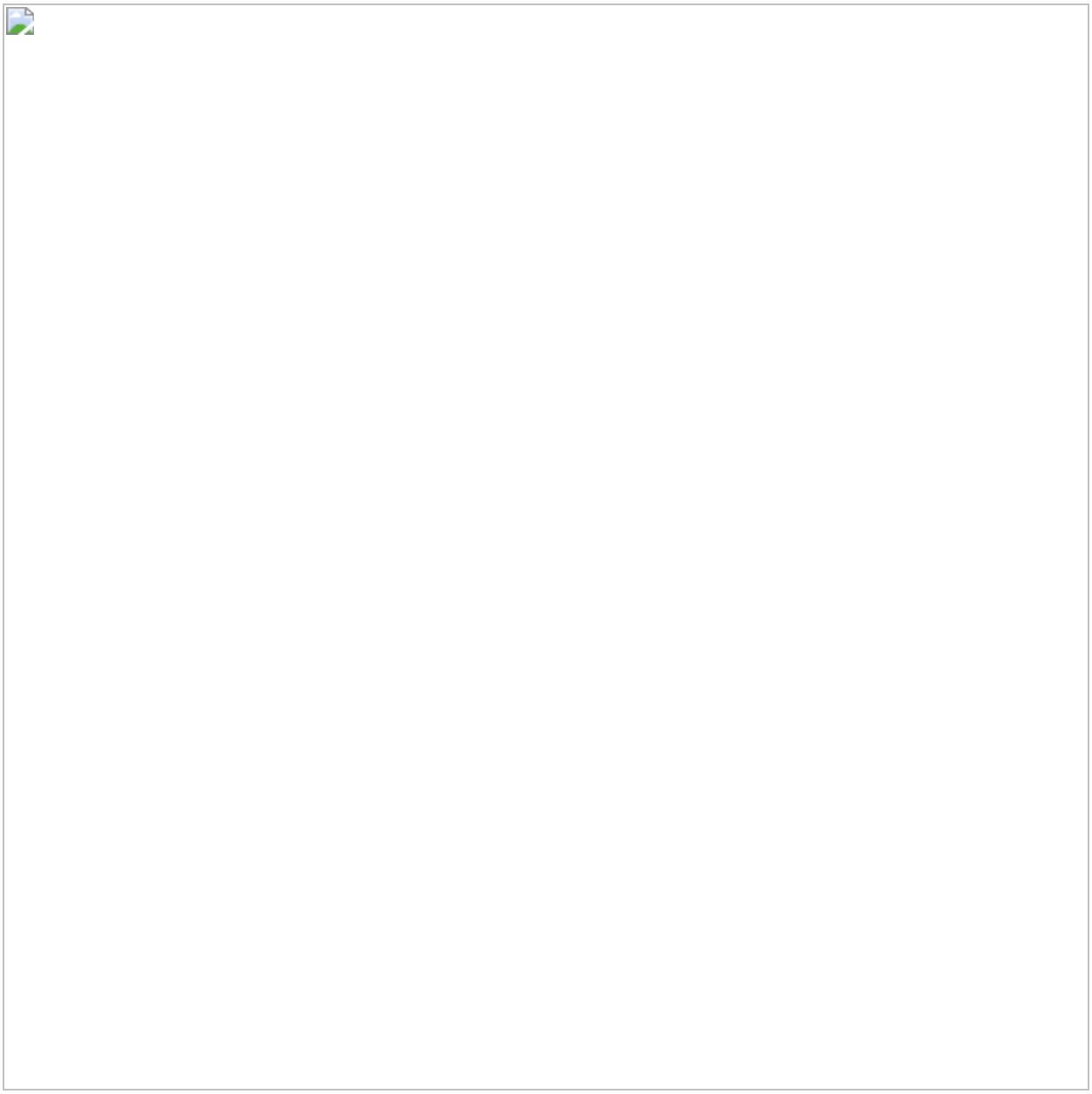
Tinba's new behavioral changes include:

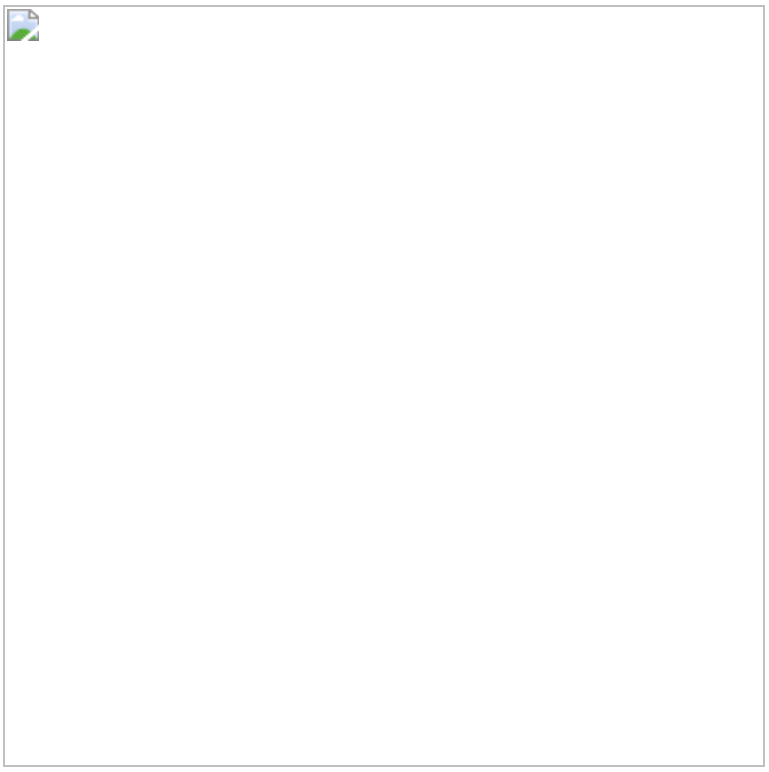
- **Domain Generation Algorithm (DGA):** Refers to a fallback mechanism for a bot to "call home" in case of the original C&C has been taken down.
- **Public Key Signing:** Refers to a verification mechanism guaranteeing that a message could only be sent from authentic bot herder.

- **Preloaded Configuration:** The malware is configured to attack at time of infection (even with no C&C connectivity).
- **Advanced Encryption Methods:** An additional (machine-dependent) encryption layer has been added.
- **User-Mode Rootkit Capabilities:** A means of hiding its traces and evading detection, even from advanced users.

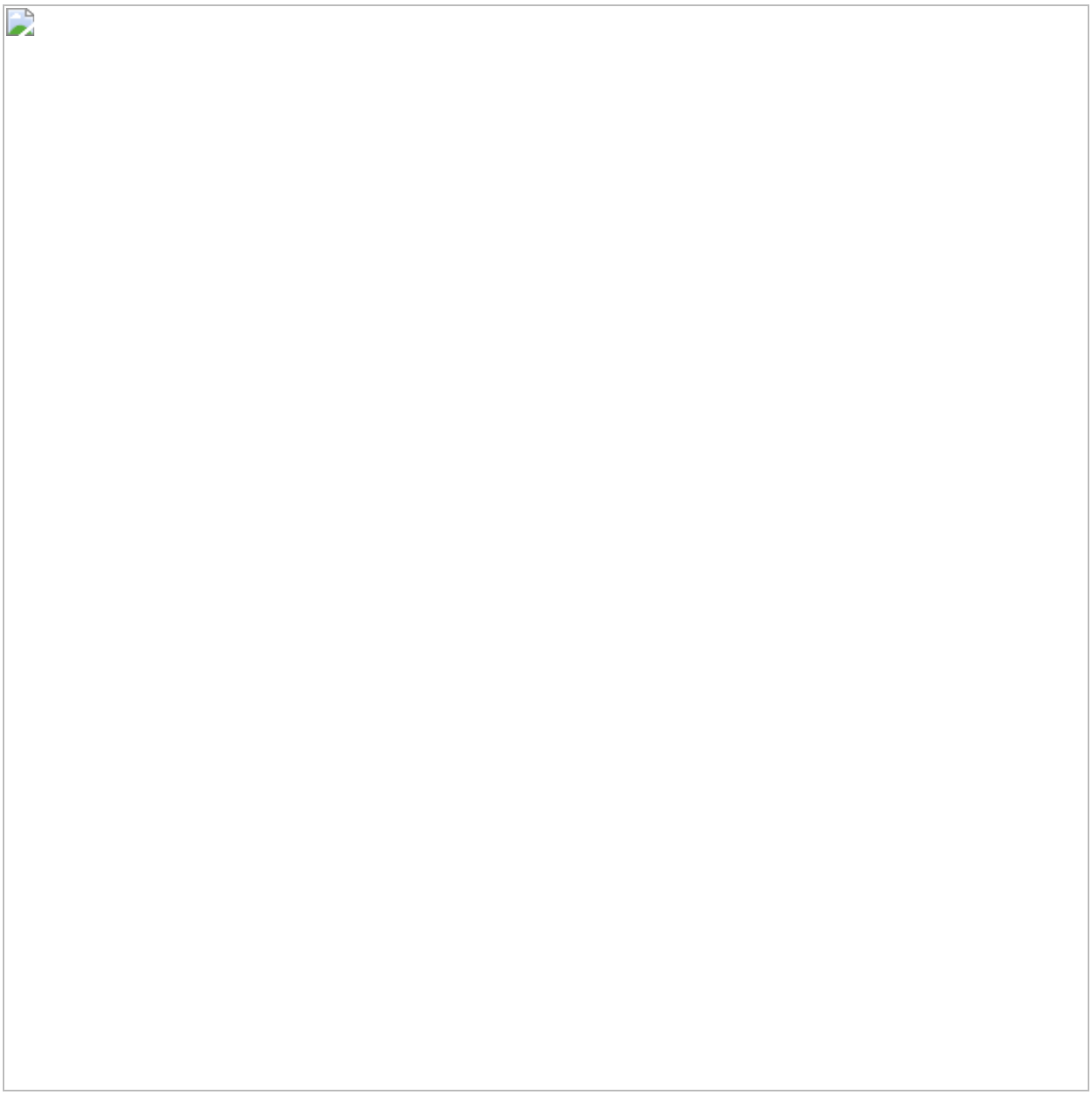
Technical Analysis: From the Dropper to the Browser

After the dropper is executed, it generates a folder name using a hard-coded key XORed with the machine's volume-serial number. The resulting hexadecimal string is used both in the malwares' folder and mutex names. (The malware executable file name is hard-coded and hasn't changed since the original Tinba).



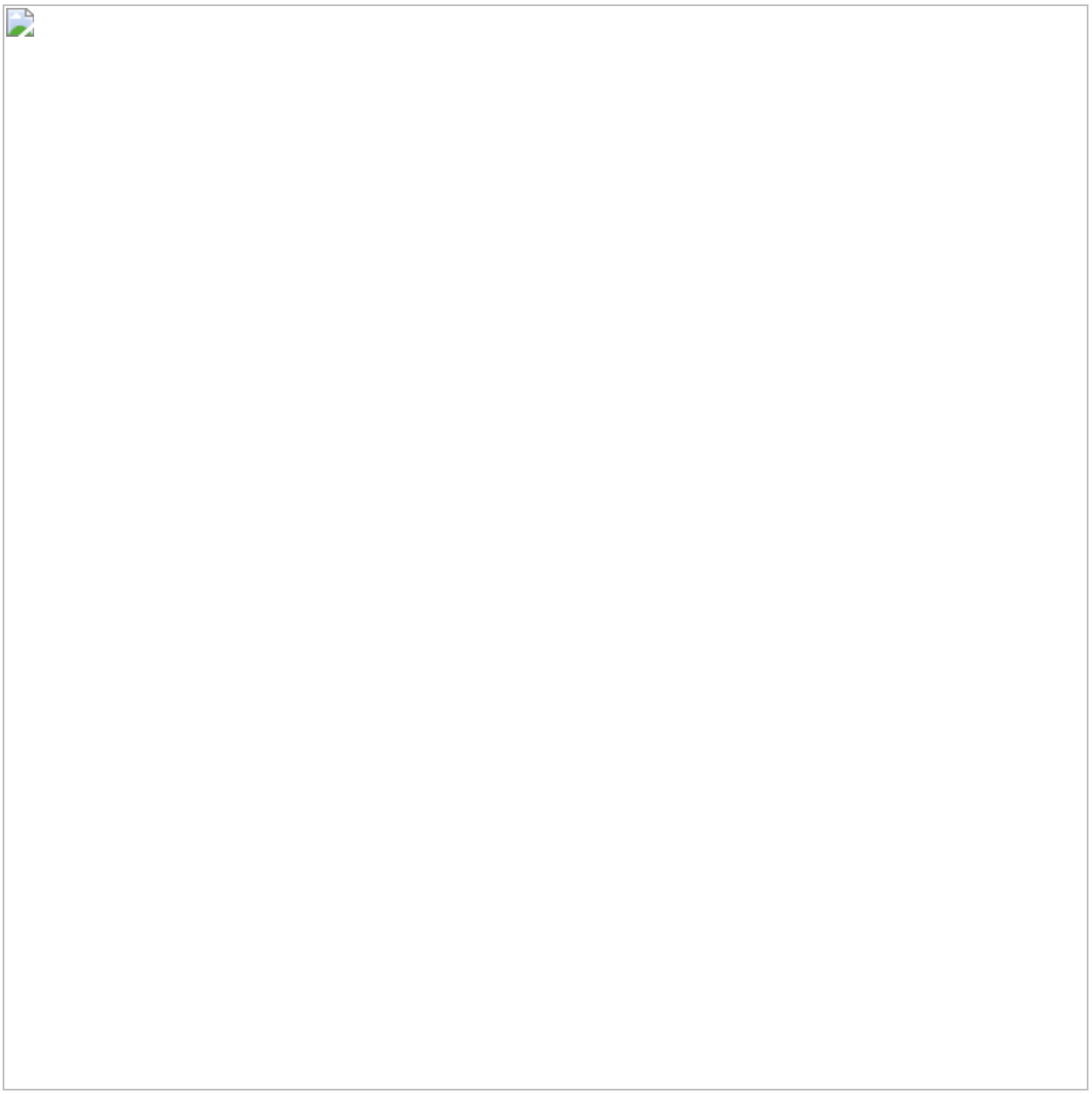


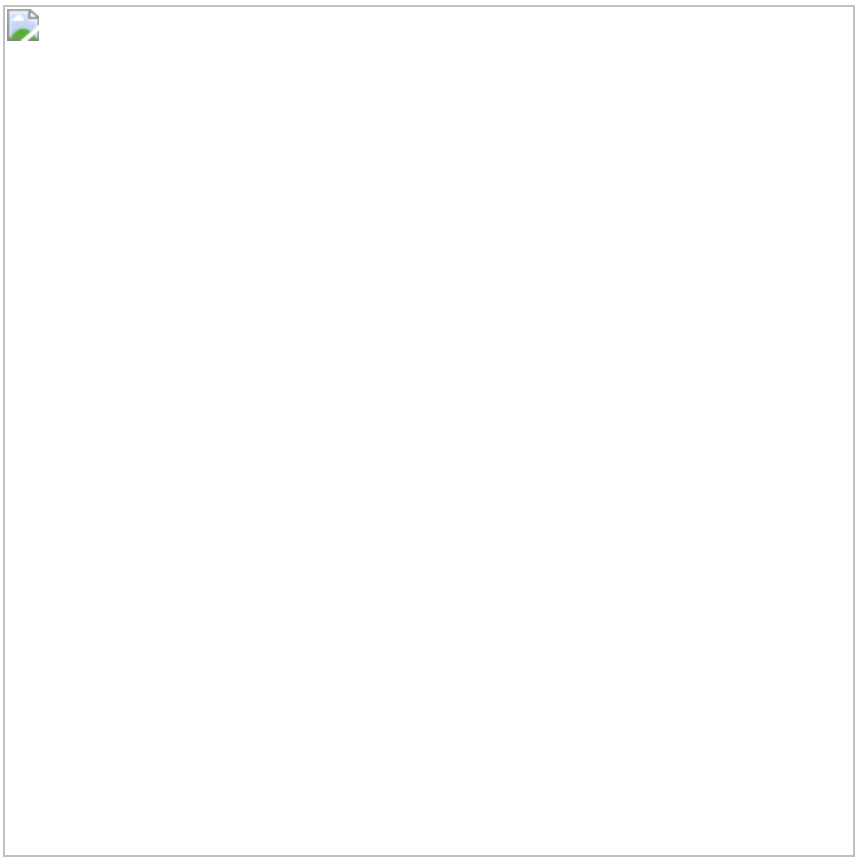
Following that, the malware installs hooks on functions such as NtResumeThread, NtCreateUserProcess and NtCreateThread, which allow it to stealthily propagate in the system. Furthermore, it hooks NtQueryDirectoryFile and NtEnumerateValueKey in order to hide its folder and run key from advanced users.



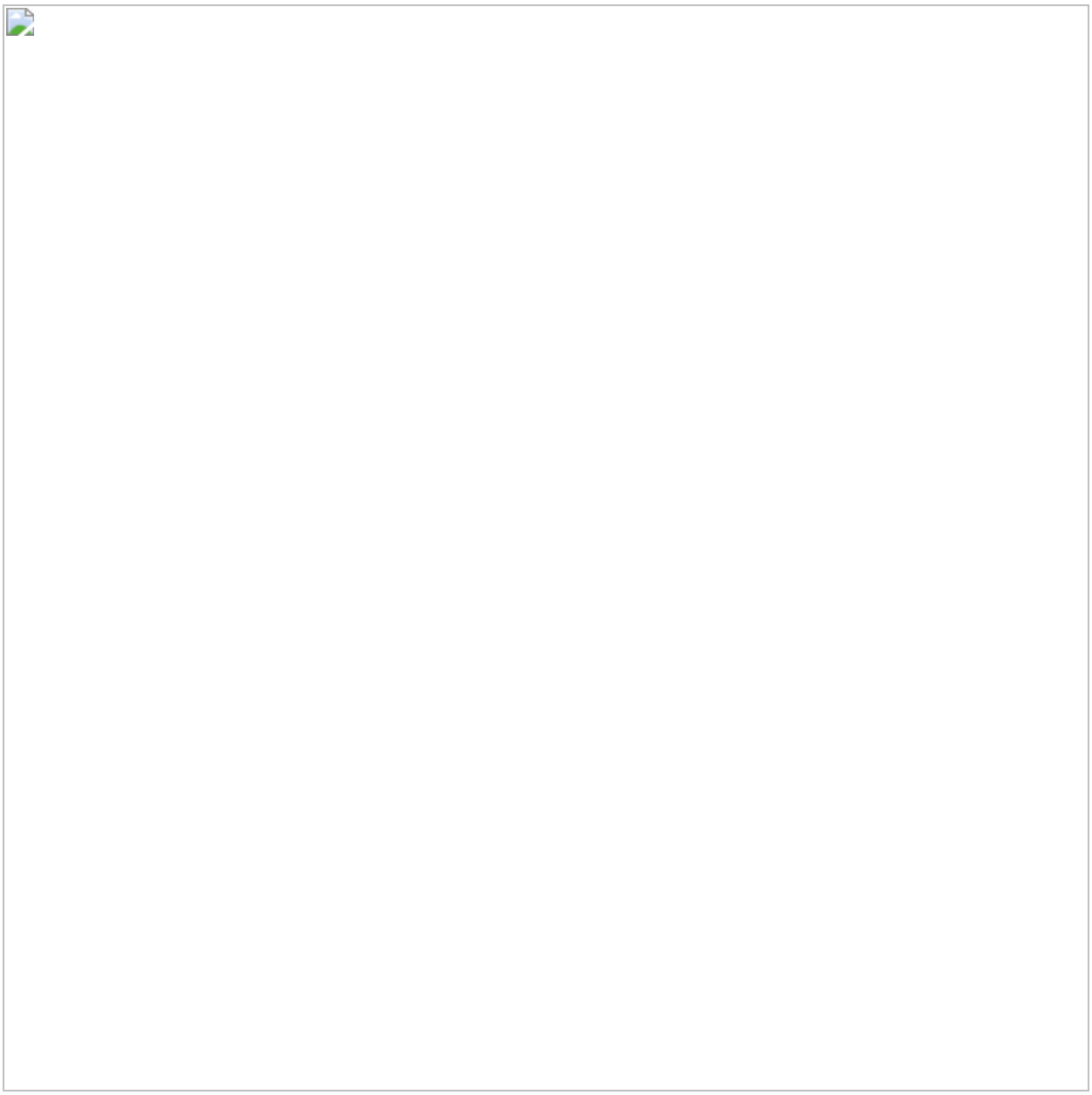
Tinba Malware Phones Home

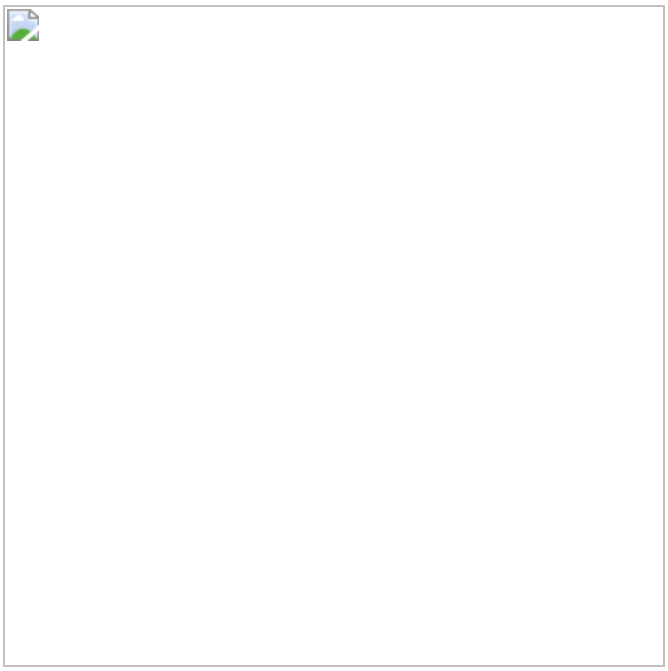
Tinba is joining Gameover Zeus in an attempt to improve communication capabilities with the C&C by having a fallback in the form of a DGA. Initially, it attempts to communicate with a hard-coded C&C server, and in case of failure, it starts using one of its fallback-generated domains.

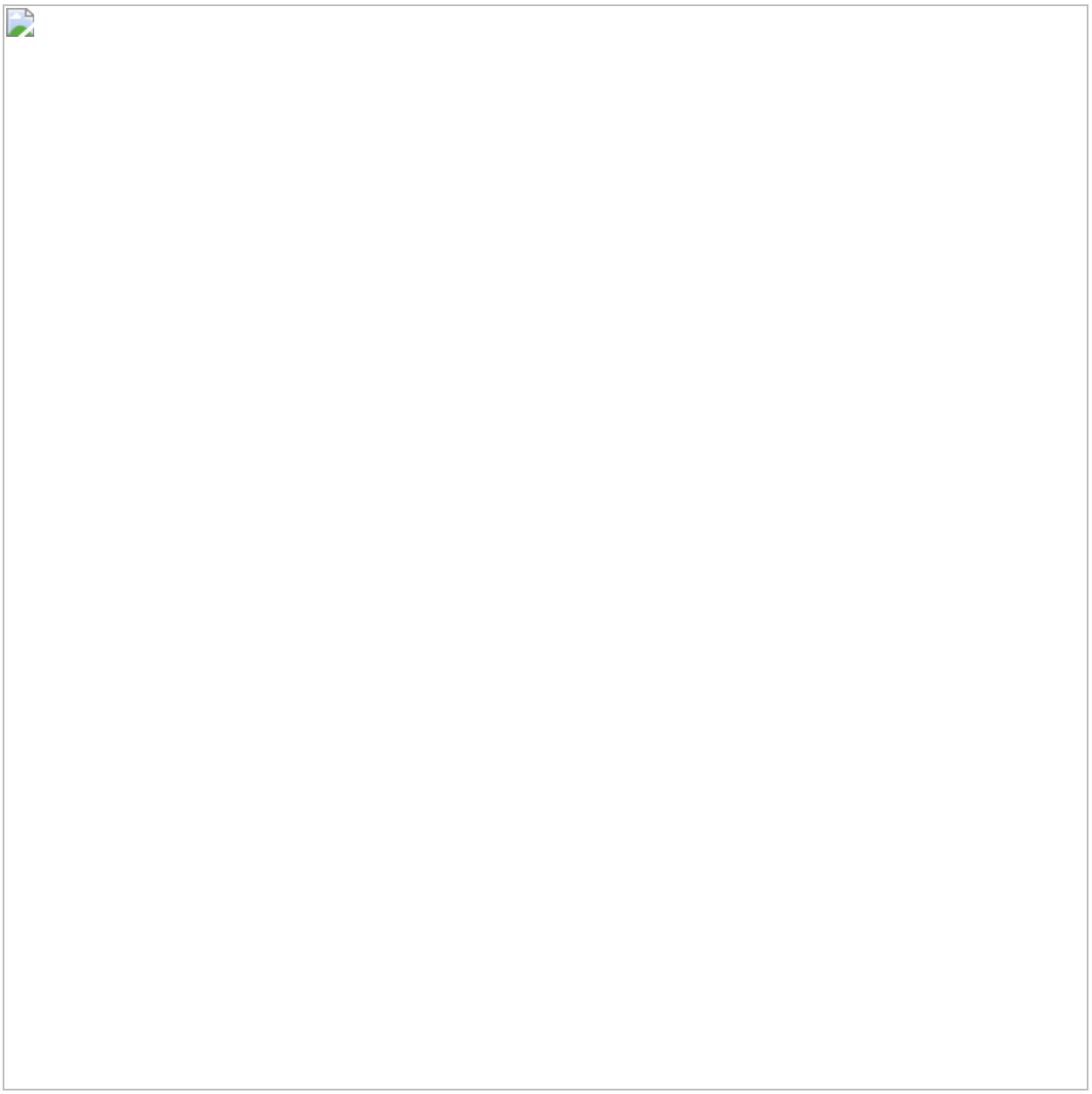




An additional feature of the new strain is the usage of the crypt32 Windows library in order to authenticate the server against a challenge response. The infected machine sends a request comprising several time stamp counters (counting the number of CPU cycles since reset) concatenated together. This technique ensures a unique challenge is sent every time, so intercepting one challenge does not suffice to impersonate as the C&C server. This message is encrypted with RC4 (like all of Tinba's communication) and then sent to the server. A hash of the message is created using SHA-1. The hash is then encrypted with a private key on the server's side and returned as part of the response. The response itself is authenticated by the malware using the Windows API CryptVerifySignatureA with a hard-coded public key.







It is important to note that without proper authentication, the communication routine will not continue, and the authentication process will repeat forever. Following a successful authentication, the communication routine repeats itself several times and then attempts to authenticate again. This is done in gradually expanding intervals.

Configuration

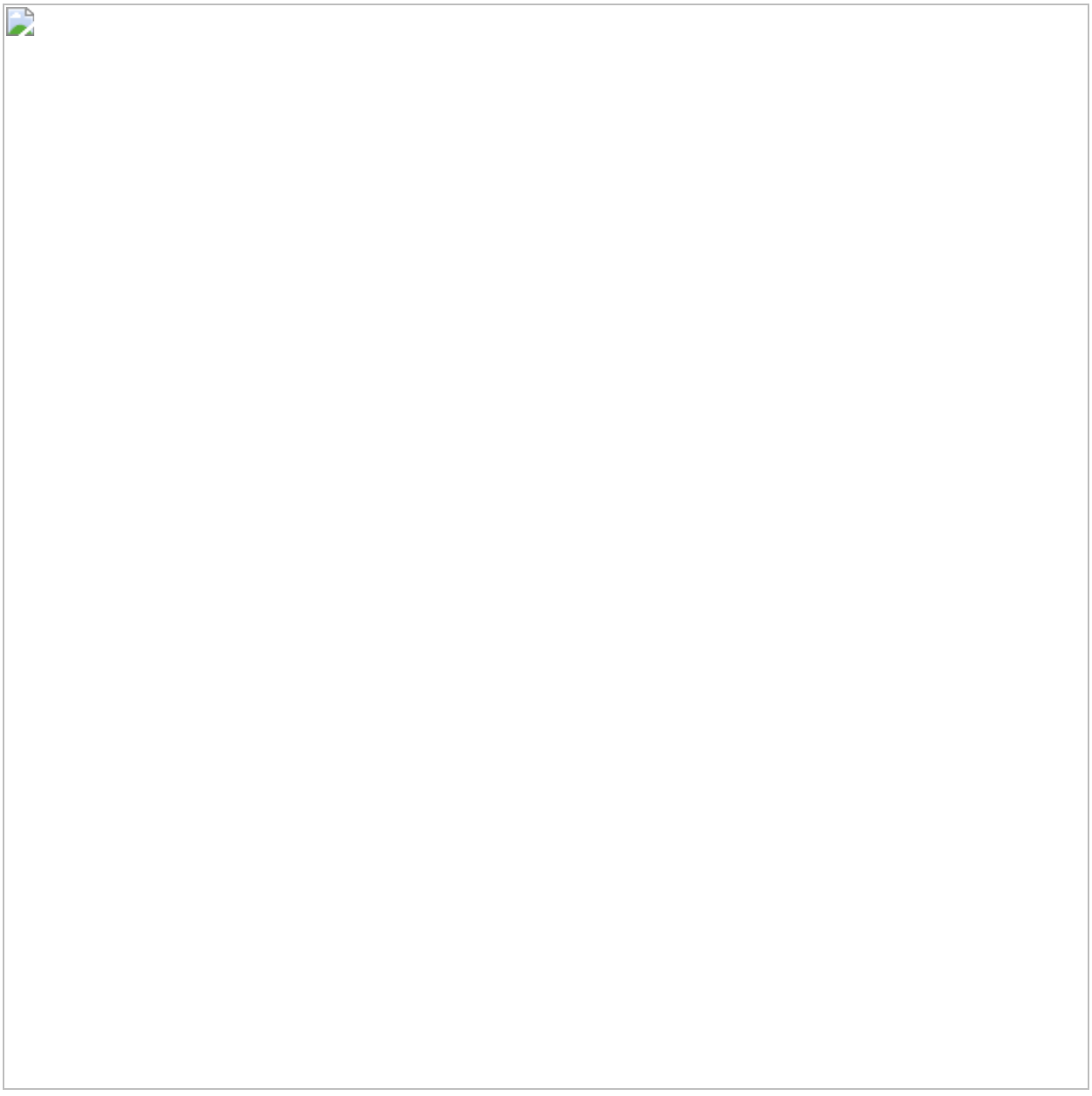
As opposed to previous Tinba strains, the new one comes with a preloaded configuration. If the browser is launched while the malware was unable to download a configuration, the preloaded, hard-coded one will be used instead.

In addition, on top of the RC4 decryption layer used in previous strains, the new strain adds a pre-step of XOR with the volume serial and a post-step of decompression using aPLib.

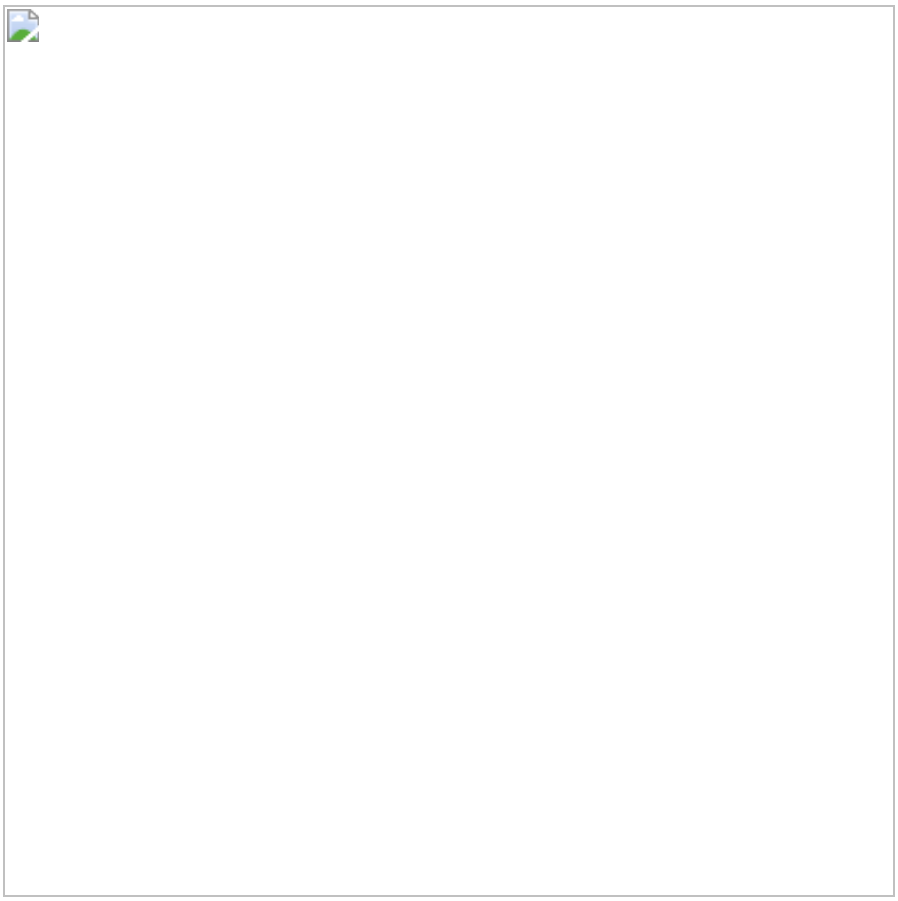
Automatic Transfer System Engine

In some recent configurations, we've discovered an interesting gem: the use of an ATSEngine panel, similar to the latest versions of Zeus, such as Citadel and ZeusVM.

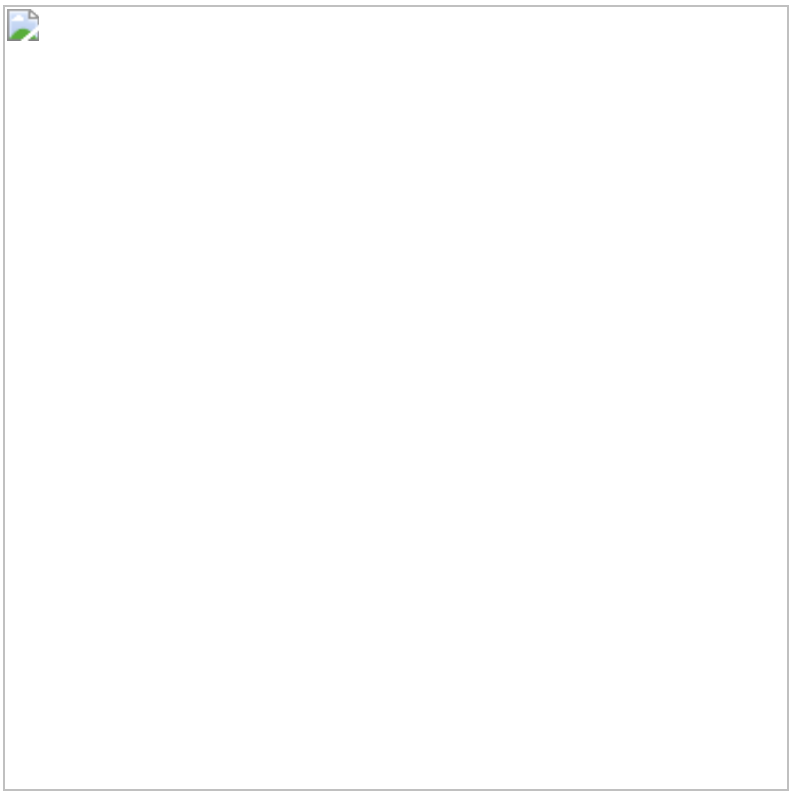
Tinba configuration contains webinjects of external malicious Javascript code, as seen below:



This malicious code is capable of applying dynamic webinjects in a large number of online banking websites. It adjusts the webinject to the exact look and feel of the original website.



These dynamic webinjects are part of the ATSEngine infrastructure that enables the attacker to collect multiple data elements, such as the victims' credit card type (credit, debit), CVV, PIN and SSN. The fraudster can then use a man-in-the-browser attack to transfer the available balance to a third party (a money mule), who withdraws the funds and sends them to the attacker in an untraceable way.



Sample MD5s

MD5	First seen	Campaign
29f83c2c462deac10f3d06c42cc82f7e	09/09/14	Canadian
f5b486f92d336a5f3385314a70373ded	30/08/14	Global
bc6ede0ee763a67a016642f737d07bd6	28/08/14	Global

Conclusion

Since the Tinba source code leak in July, Tinba has been spotted in various locations across the globe with new features and functionality. This serves as a reminder that cybercriminals are fully aware of reverse engineers and researchers analyzing their products; they are constantly developing new tactics and methods while attempting to stay under the radar and bypass automated and human security controls.

IBM Security Trusteer researchers and threat analysts are closely monitoring this variant while providing appropriate protection against this new threat, using either IBM Security Trusteer Rapport or IBM Security Trusteer Pinpoint Malware Detection to provide protection against this type of financial malware and many others. These solutions can detect, mitigate and remediate infections to protect the enterprise and your customers.

Assaf Regev

Assaf Regev serves as the product marketing manager for the web fraud portfolio of Trusteer, an IBM Company, part of IBM's Security Systems division. Assaf...


IBM Security