

The Crimeware Ecosystem

By Ryan Sherstobitoff



One could never have imagined the evolution of crimeware over the last couple of months following defined patterns within an established ecosystem. Malware creation groups now follow the model and organization of their legitimate counterparts, finding every way possible to make profit.

A year or so ago the very nature and principles of malware creation shifted, evolving to being economically driven. Several stages within this evolution have contributed to the present cybercrime landscape:

1. A shift from curiosity to profit
2. Malware creation becomes organized towards one goal: financial gain through illicit means
3. Malware authors follow common trends in business and commerce to take advantage of their victims (i.e., iPhones, etc).
4. The first ever cybercrime-for-sale products are available through various Russian hacking forums
5. Malware authors saturate security labs with an ever increasing pace of new malware, creating sustained denial of service against resources
6. Targeted attacks focusing on specific user populations, entities – monster.com, facebook, salesforce.com, etc. – increase
7. Banker Trojans emerge, utilizing complex means of injecting HTML into browser sessions to capture credentials
8. Banker Trojans evolve to include capabilities of diverting funds in mid-flight and hiding the actual code within a remote server in the cloud

For example, a high volume of banker Trojans are currently affecting consumers abroad using a wide range of techniques to capture confidential information associated with banking such

as pin numbers and other data. This information is then used illegally in several ways: credit card scams, printing fake ATM cards, purchasing goods with stolen credit cards and then selling at discounted prices, and a host of other scams.

These Trojans are designed to work with the authentication mechanisms incorporated by the bank. For example, a number of Trojans inject non-existent fields into the live banking session to capture additional information the bank normally would not ask for. There are even cases of Trojans hi-jacking sessions in real time and sending funds to accounts other than originally intended.

While this may seem to be a bleak outlook in regards to the current state of affairs, it happens to be the reality that we live in today.

You may be asking at this point, just how widespread is this problem? The fact is that over 50% of the detections within our labs are related to Trojans – mostly banker Trojans – designed to steal confidential information.

The methods and vectors for attack have also evolved from the early simplistic means (email or very basic phishing) to complex targeted attacks with multiple vectors in play. We can also see there has been an evolution from the basic common to the complex targeted delivery mechanisms:

1. Network self-propagation as seen in complex network worms such as MyDoom, Blaster, Sasser, etc. These worms were seen at the tail end of the massive epidemics at the end of 2004 to early 2005.
2. Malware propagation through email attachments, mime vulnerabilities, etc.
3. Basic email phishing campaigns targeting specific banks, usually PayPal, Bank of America and host of Euro-

pean and Brazilian banks

4. Targeted “spear” phishing campaigns focusing on specific entities and specific user populations

5. Lacing legitimate web-sites with iFrame tags referencing several MPack servers.¹

IT Security vendors at one point warned customers against visiting “the dark side” of the Internet in order to avoid becoming infected; thus, a whole business of Internet content filtering was established to help organizations enforce acceptable use policies.

However, this warning is no longer valid as a many legitimate sites are now being compromised in order to be a staging ground for malicious code attacks. This quick and dramatic change in the last year has rendered traditional security defenses (firewalls, IPS, antivirus, etc.) ineffective in terms of combating this new generation of malware. Statistics show that up to 72% of companies today are likely to be infected with undetectable threats.

We can conclude that the malware authors quickly adapt to changes in the economy and the defenses put in place to mitigate or eliminate their activities.

About the Author

Ryan Sherstobitoff is the Chief Corporate Evangelist at Panda Security USA (www.usa.pandasecurity.com). Ryan lectures across the USA on cybercrime trends as well as corporate risk assessments. He can be reached at ryans@pandasecurity.com.

¹ MPak is a full-featured malware kit sold through the underground economy. Installed on a server, it allows malware to be run on remote systems. See <http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf>.