TREND MICRO™ | Securing Your Web World

Observations on Emerging Threats

Paul Ferguson
Threat Research
Trend Micro, Inc.
Cupertino, California USA

5th USENIX Workshop on Large-Scale Exploits and Emergent Threats
LEET '12
Botnets, Spyware, Worms, New Emerging Threats, and More
APRIL 24, 2012
SAN JOSE, CA
usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Trend Micro Threat Research

“Trend Micro's Threat Research group is specially tasked with looking forward on the threat landscape and working with technology and/or various product development groups inside the company to ensure that, as a company, we deliver the appropriate security solutions to address emerging threats to our customers. To accomplish this requires our threat research group to understand, explore, and deconstruct various malicious technologies, campaigns, vulnerabilities, and exploits which are currently being perpetrated on victims today.”

TREND MICRO

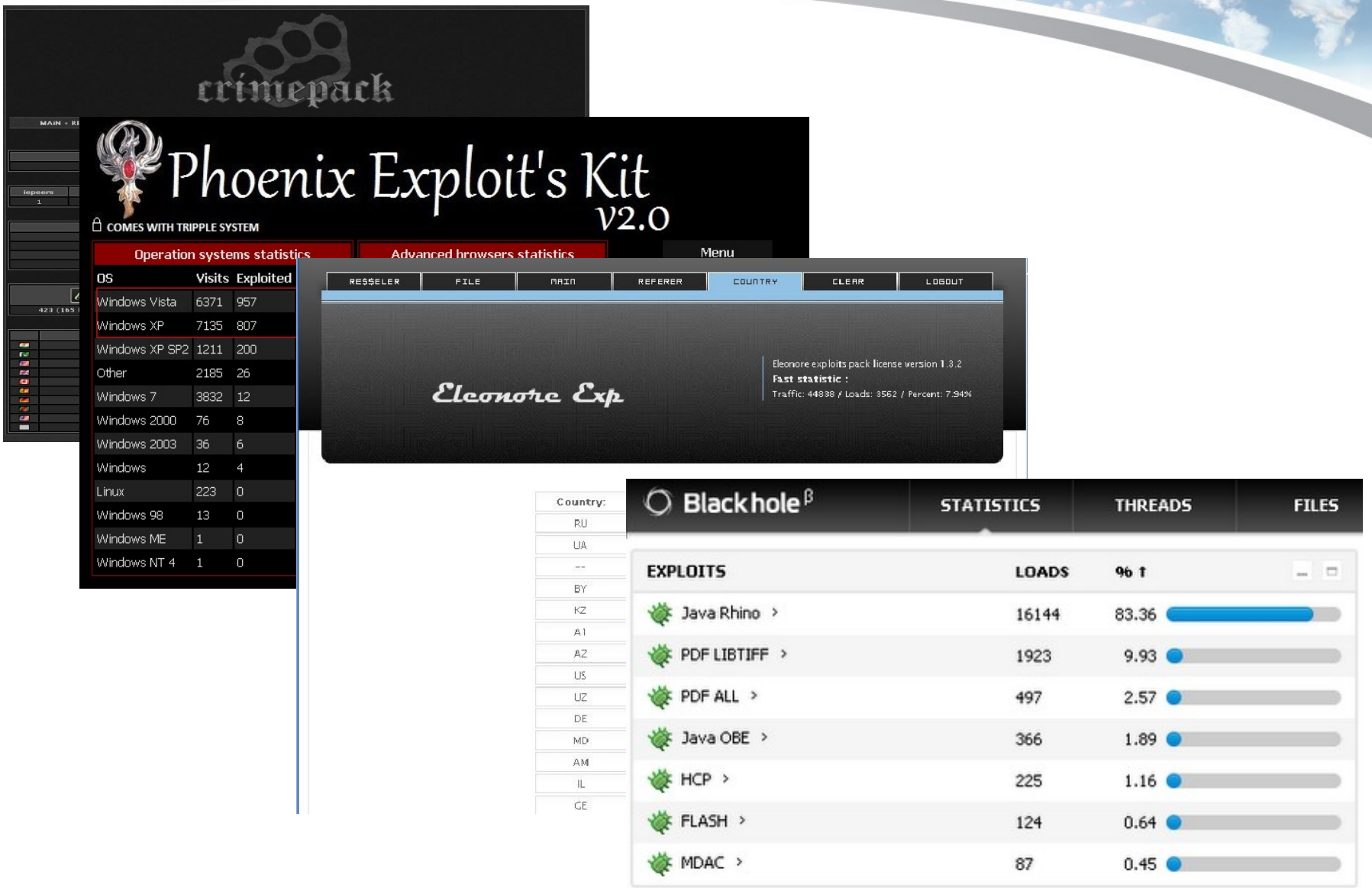
Introduction

- Evolution, Commoditization, Professionalism of Exploit Kits
- Increasing Sophistication of Traffic Direction Systems (TDS)
- Smaller, Diversified Botnets
- Modularization
- Evolution of Mobile Threats
- Continued Exploitation of Social Networks
- Critical Infrastructure Attacks
- HTML5 “Exploitation”
- More Data Breaches via Targeted Attacks (APT)
- “Hard-to-Reach” Relocation of Criminal Activity

TREND MICRO

Evolution, Commoditization, Professionalism of Exploit Kits

- Virtually **ALL** “Professional” Eastern European criminals are using various Exploit Kits to increase the possibility of successful compromise.
- Generally used only by Eastern European criminals.
- Example Evolution: Crimepack → Phoenix → Eleonore → Blackhole
- Each step of evolution is an incremental improvement on previous iteration.
- Blackhole Exploit Kit is currently the most popular kit.
- Uses heuristics to determine what vulnerabilities may exists on the end-system to determine what payload to deliver.



TREND MICRO

Increasing Sophistication of Traffic Direction Systems (TDS)

- TDS are used to redirect a victim to specific landing page – based on some criteria (below).
- Redirection criteria is generally referrer (affiliate ID).
- Primary used to direct traffic by pay-per-install or pay-per-click campaign in order to manage monetization scheme(s).
- Manage/Tracks Statistics, e.g. Hits, By Country, Referrers, etc.
- Currently Most Popular: Sutra TDS
- TDS are generally used to redirect victim to an Exploit Kit, Fake AV, etc., depending on affiliate campaign.

Traffic statistics generated by SUTRA
(Sun Jun 13 13:05:02 2010, SCHEME: **3**)

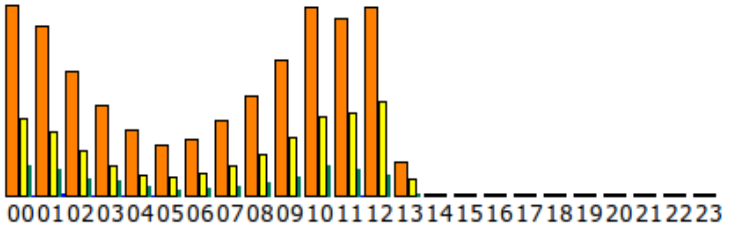
2010/06/13

Referers , Countries and Ager

Referers	Raw hits	Unique hits
http://media-click.ru/stat.php?id=648	7590	1297
http://xxlib.org/	6253	2837
http://protizer.net/new__stat.php?id=5422	4576	2875
http://protizer.net/new__stat.php?id=1944	4081	2965
http://media-click.ru/stat.php?id=6306	2566	700
http://protizer.net/new__stat.php?id=10115	1922	1488
http://micro-win.com/	1290	347
http://protizer.net/new__stat.php?id=1166	844	602
	801	184
http://protizer.net/new__stat.php?id=23633	712	372
http://protizer.net/new__stat.php?id=17490	677	422
http://hitlife.net/sex_online_game/	659	188
http://protizer.net/new__stat.php?id=7544	651	439
http://media-click.ru/stat.php?id=5317	641	205
http://protizer.net/new__stat.php?id=286	508	385
http://protizer.net/new__stat.php?id=18872	443	272
http://protizer.net/new__stat.php?id=2732	437	231
http://micro-win.com/index.php	390	68

Cod				
RU				
--				
US				
UA				
DE				
KZ				
TR				
LV				
BY				
IL				
MD				
CA	Canada	132	0	20
PL	Poland	125	0	27
CH	Switzerland	115	0	4
FR	France	109	0	16
NO	Norway	106	0	21
IE	Ireland	97	0	5

top 'Raw hits' = 6662



Hour	Raw hits (■)	Uniques (■)	Proxies (■)	Without referer (■)
total	57629	23617 (41.0%)	9599 (16.7%)	801 (1.4%)
00	6662	2684 (40.3%)	1141 (17.1%)	110 (1.7%)
01	5939	2229 (37.5%)	1005 (16.9%)	154 (2.6%)
02	4342	1535 (35.4%)	721 (16.6%)	95 (2.2%)
03	3188	1030 (32.3%)	664 (20.8%)	81 (2.5%)
04	2290	732 (32.0%)	462 (20.2%)	96 (4.2%)
05	1756	637 (36.3%)	288 (16.4%)	8 (0.5%)

Smaller, More Diversified Botnets

- Decline of Large, Monolithic Botnets (e.g. Storm, Conficker, Waledac, etc.)
- Diversification as a result of take-downs impact
- Bot infrastructure is “cheap” but seeding takes time
- Most of the time & effort is in the seeding, e.g. Initial spam runs or drive-by (or exploit kit) campaigns, etc.
- Banking Trojan Botnets are a great example: Customization by Each “Owner/Operator”, hundreds of individual “botnets” may exists in parallel.

Emergence of Modularization

- Banking Trojans Modularization: Screen Grabber, Back-Connects, Web Injects, etc.
- Exploit Kit Modularization: Modules added for new exploits (per-CVE/Exploit, per-browser, per-plugin, etc.)
- We expect to see further evolution of the modularization concept in new “plug 'n play” Trojan and exploit kits, as well as other platforms.

Evolution of Mobile Threats

- Most Mobile Threats thus far can be considered “Proof-of-Concept”
- Majority have been legitimate Apps which have been Trojanized
- Majority have been re-packaged Trojan Apps that appear in “illegitimate” App markets.
- “Professional Criminals” will ramp up targeting of Mobile platforms with wider adoption of e-Commerce Applications, Near-Field Communications (NFC), etc. where money can be stolen or redirected.

TREND MICRO

Social Network: The Low-Hanging Fruit

- Social Networking platforms allow criminals unique opportunities to get close to their victims.
- Users generally publish too much personal information on Social Network platforms which can be used against them in a criminal campaign.
- Humans are generally naive, too trusting, easily baited, tricked, fooled, or just plain thoughtless and reckless in their online behavior.
- No obvious reason to think that this will change.

Critical Infrastructure: Some Hard Lessons Will be Learned

- Just like other private networks, many (most?) connected to the Internet in some way.
- Just like other privately owned infrastructure, a lot of utilities/industrial control systems are not well-secured or have poor security posture.
- Transportation, Manufacturing, Electricity, Water Processing, etc.
- We expect to see an escalation of security incidents involving “critical infrastructure”, and perhaps some serious reconsideration of how these systems are connected to the rest of the world.

New Exploitation Vectors with HTML5

- With HTML5, attackers can now create a botnet which will run on any OS, in any location, on any device.
- HTML5 is heavily memory-based, barely touches the disk, and may be difficult to detect via traditional antivirus.
- More enabling of XSS, Click-jacking, Tab-Napping, CSRF/CSOF
- Web Sockets allows surreptitious delivery mechanism for malicious content (exists today with Flash).
- Similar in fashion to JAVA, more ubiquitous adoption of HTML5 will help foster a more homogenous attack surface.

More Data Breaches via APTs

- Data Breaches via “Targeted Attacks” or “APTs” share many similar foundations in human behavior, trust, and susceptibility to being “socially-engineered” – these will continue to proliferate due to the ease in which they can be executed by determined attackers.
- Observation: Virtually ALL of the **successful** targeted attacks we have observed have used very simple social-engineering tricks.
- Once attackers have successfully gained a presence, they use various modified programs to mover laterally, find targeted resources, and exfiltrate data.

TREND MICRO

Criminals Move To More 'Resistant' Services

- Professional criminals (especially) have refined the art of “maximizing their windows of opportunity”.
- They learn which services allow them the maximum amount of maneuverability and long-lived operations (protection to operate).
- Observation: Criminals already know which hosting providers, domain registrar/reseller, upstream connectivity, etc., provides them the most “window of opportunity”.
- As some emerging economies become more connected to the Internet, there is generally a lag between connectivity/services and security “policing”. We predict the Africa continent, as it becomes better connected to the rest of world, will be a haven for criminal hosting.

TREND MICRO

Summary

- “Snapshot in time.”
- ***“...wait 15 minutes and it will change.”*** Weather colloquialism.
- The biggest challenge for any organization is to adapt quickly to a changing threat landscape. Be nimble.
- Threats manifest themselves in the most bizarre, and sometimes mundane, ways.

TREND MICRO

TREND MICRO™