websense®

APT or Targeted Attack, What's the Difference?

Michael Cryer,

Consulting Systems Engineer

websense®

Michael Cryer, CISSP

Consulting System Engineer

- 4 Years at Websense
  - General Sales Engineering & Research
    - Member of Satellite Research Team (Websense Security Labs)
    - Advanced training and sales methodologies for technical Sales Engineers
- 5 Years at PricewaterhouseCoopers
  - Lead Northeast practice for forensic investigations
    - Certified Forensic Investigator: TJX, BJ's Wholesale, and several fortune 100 companies
    - Analyzed data breaches & provided recommendations for remediating risk
  - Member of Attack and Penetration Core Team
    - Developed attack strategies and assessment methodologies

websense®

What is an APT or Targeted Attack, and why should I care?

TRITON™

- Web security
- Email security
- Data security

Advanced Persistent Threats

websense®

Advanced Persistent Threat, n.

"A group, such as a foreign nation state government, with both the capability and the intent to persistently and effectively target a specific entity." (Wikipedia)

Advanced Persistent Threat, n.

"Really nasty malware." (Everybody Else)

APTs are all over the news

websense®

Major attacks last 18 months

websense®

- **January 2010** – Aurora hits Google, Adobe and 30+ large organizations. Used 0-day in IE.
- **March 2010** – NATO announces that they've seen a significant increase in cyberattacks against their network in the last 12 months
- **April 2010** - Attackers gain access to systems within the Indian Defense Ministry and Indian embassies around the world.

Major attacks last 18 months

websense®

- **September 2010** – Stuxnet, a highly advanced and targeted malware, was found. This was the first malware to specifically target critical infrastructure, in this case a nuclear facility in Iran.
- **February 2011** – Night Dragon is announced. Targeted attacks against oil, energy and petrochemical companies
- **March 2011** – RSA reports they have been a target of an APT using a 0-day in Adobe Flash coming via attached XLS file.
  - Stolen RSA Token algorithm was later used on specific targeted attacks vs. US Defense contractors

The big picture

websense®

- APT is just a buzzword
  - These types of attacks have been around for over 5 years
  - The majority of these targeted attacks use re-packed versions of existing, well-known Remote Access Trojans (RAT's)
  - They happen almost daily.
  - Security vendors and the media are creating cool names for groups of attacks (it gets a lot of attention).

Whether an attack is an APT or not, this is simply a matter of semantics, and REALLY doesn't matter if you are the one under attack.

APT or targeted attack?

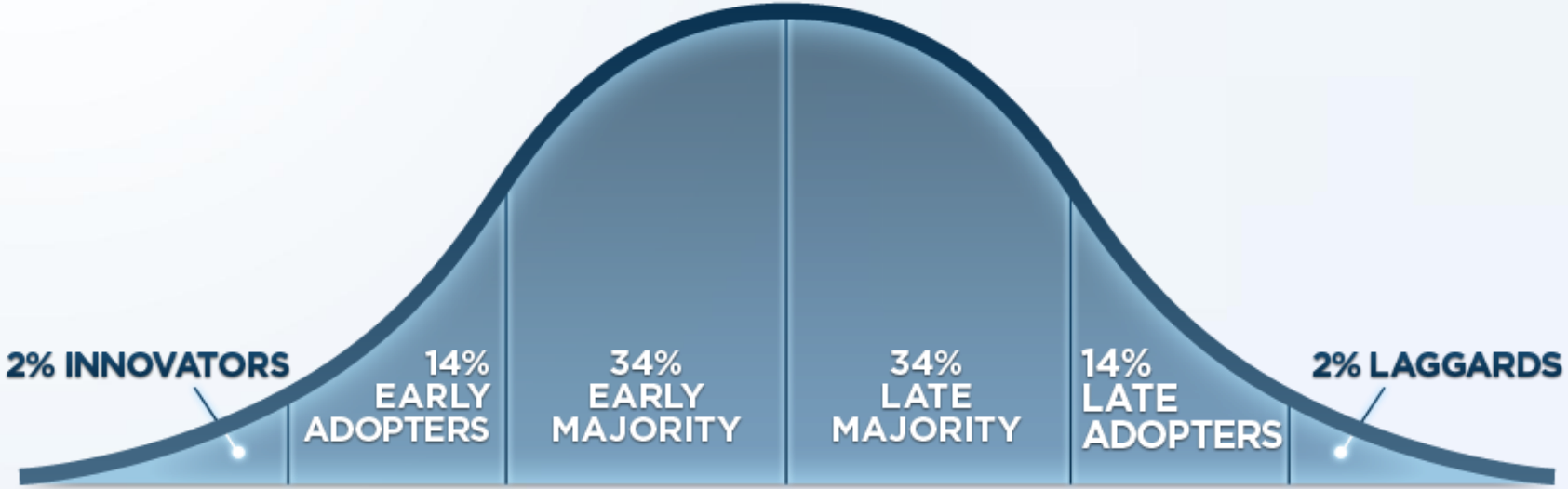
websense®

Advanced Persistent Threats Example: Aurora	Characteristics	Targeted threats Example: Epsilon
Leveraged an unknown Internet Explorer vulnerability using malware binaries and a backdoor connection that masqueraded as an SSL connection to command and control victims' servers	**Sophistication** Uses the full spectrum of attack methods, including email phishing, website malware, Trojan downloads, and more	Used social engineering to send emails that enticed employees to open an Excel file that contained a Flash vulnerability
Targeted Google and dozens of other major corporations, including Adobe Systems, Yahoo, Morgan Stanley, and Dow Chemical	**Specificity** Targets a particular entity and has a specific mission to accomplish, typically of a military, political, technical, or economic nature	Targeted a major email marketing company whose customers included Visa, Kraft, and Marriott International
Custom-built to exploit an unknown vulnerability in Internet Explorer, thus evading traditional security measures with a "zero-day" attack	**Specially designed** Custom-built for specific purposes; often a first-of-its-kind exploit that's never before been seen or detected	
Masterminded by the Chinese government to locate, steal, and modify source code repositories at high-tech, security, and defense contractor companies	**Sponsorship** Backed by governments, organized crime, or other entities with deep-pocket funding; managed by well-organized "crews" with highly coordinated assignments to accomplish	

- Are all attacks APTs?
  - Some are, but most are not
  - The business impact is real either way
  - The attacks need blended defenses, one single technology won't stop it
- Targeted attacks
  - Majority of attacks don't use a 0-day vulnerability
  - The attacker very often uses a repacked version of a well-known Remote Access Tool
    - Poison Ivy, Gh0stRAT, zwShell
  - Even if re-packed the communication protocol stays the same (HTTP/s)
  - Often connect to Dynamic DNS hosts

Malware Adoption Lifecycle

websense®



Where is the data sent?

websense®

- China in many cases, sometimes North Korea
- C&C/data drop use Dynamic DNS hosts
  - liciayee.dyndns-free.com (CVE-2011-0611, Adobe 0-day)
  - obama.servehttp.com, prc.dynamiclink.ddns.us (RSA attack)
  - is-a-chef.com, thruhere.net, office-on-the.net, selfip.com (Night Dragon)
- Websense is adding a Dynamic DNS category which can be used to block access to websites and block data from being posted.

websense®

How do they work?

TRITON™

- Web security
- Email security
- Data security

3 Phased Approach

websense®

Attack Phase 1

PLAN, LAUNCH, INFECT / SUCCESS	The initial phase is when the attacker performs some sort of reconnaissance, launches and attack, and then infects hosts within the target environment.

Attack Phase 2

CONTROL, DISCOVER, PERSIST	The second phase is post infection. The attacker now will be controlling the infected hosts, updating the code, and discovering other machines and data on the network.

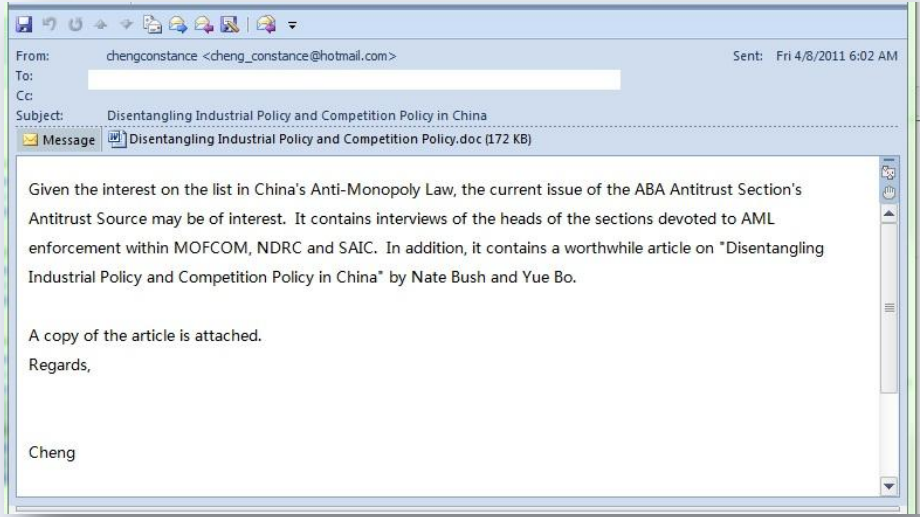
Attack Phase 3

UPLOAD, UPDATE, TAKE ACTION	The final phase is when the attackers have captured data and are uploading it and then taking action on the data.

Phase 1 - PLAN, LAUNCH, INFECT / SUCCESS

websense®

- Reconnaissance & launch of Attack
  - Email campaigns, IM Links, Malicious Web sites
  - Social Networks
  - USB Flash drives



- Exploits:
  - APT's use 0-days
    - Adobe, Microsoft, Browser Exploits
  - Targeted Attacks use repackaged known exploits that typically haven't been patched.
    - SQL Injection
    - MS, Adobe Flash, etc.

Phase 2 - CONTROL, DISCOVER, PERSIST

websense®

- Command and Control
  - Remotely update sync, modify, and send other commands to the host
  - Typically repackaged toolkits: Poison Ivy, Night Dragon, and zwShell
    - Used to download additional tools for further exploitation

- Traditional malware often will not persist on a machine, may be cleaned, remove itself or be detected and removed by an anti-virus program. Modern malware is designed to be stealthy and go unnoticed; additionally it is designed to persist back to the command and control center for updates to new undetected code to avoid detection by updated antivirus solutions.

Phase 3 - *UPLOAD, UPDATE, TAKE ACTION*

websense®

- The last phase is the ultimate goal for the attacker; this is when they steal data from the target.
  - APT attacks are looking for specific data
    - RSA – Looking specifically for Secure ID token Algorithm
      - Typically get in and out with out being detected
  - Targeted attacks typically create havoc (Anonymous)
    - Web site defacement
    - Can persist for several months/years (TJX, Sony)
    - The attack becomes public knowledge and the media publishes information about the fact
    - The attacker decides to extort the victim
    - Information about the attack is shared amongst attackers and if the attack wasn't thwarted by the victim, additional attacks from other groups take place

Packaged Tools: Poison Ivy

TRITON™

- Web security
- Email security
- Data security

Poison Ivy

websense®

- Available at http://www.poisonivy-rat.com
- Created by a Swede called “shapeless”.
  His real name is Jonas

▷ SweRAT > Viewing Profile

Viewing Profile: shapeless

shapeless

SweRAT TEAM

SWERAT TEAM

Member Group: Admin
Joined: 2005-04-17 15:47

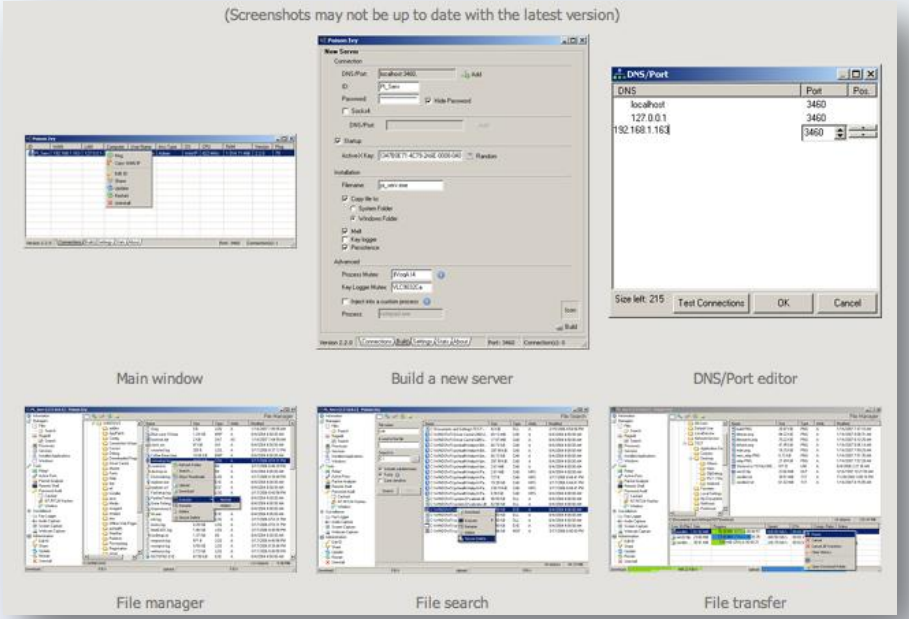
Active Stats	
User's local time	2010-12-07 02:00
Total Cumulative Posts	**1,003** (0.5 per day / 3.35% of total forum posts)
Most active in	Projekt och Releaser (161 posts / 17% of this member's active posts)
Last Active	2010-11-28 22:41
Status	OFF (Offline)

Information	
Home Page	http://www.poisonivy-rat.com
Birthday	4 Feb 1987
Location	sthlm
Interests	*No Information*

Poison Ivy

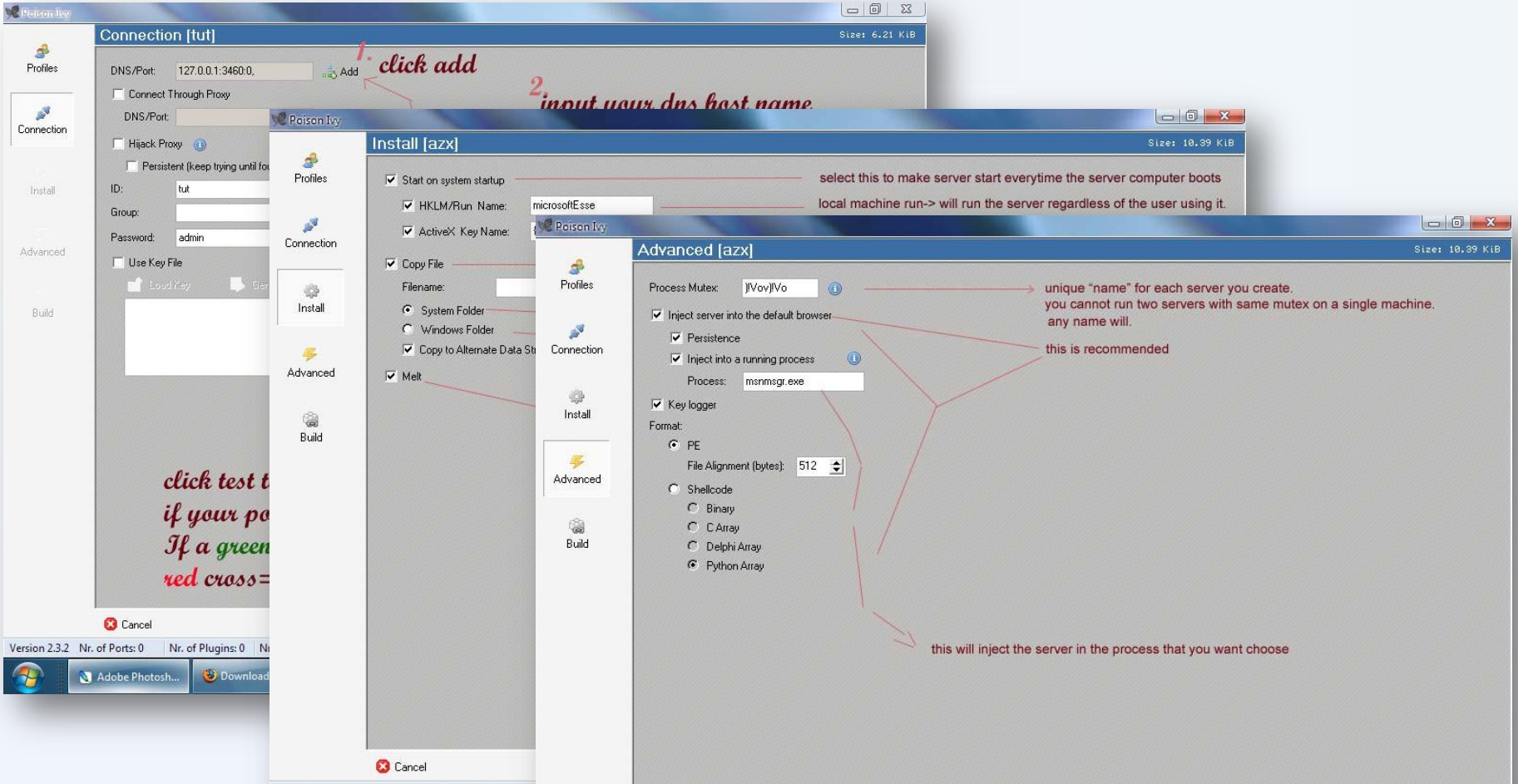
websense®

- Reverse-connection
- Keylogger
- Upload/Run files
- Remote Shell
- View/Edit Registry
- Screen/Audio capture
- Much more...



Poison Ivy Builder

websense®



websense®

How do you stop these attacks?

Preventing infiltration & Preventing data exfiltration (containment) by combining known techniques to stop blended attacks

TRITON™

- Web security
- Email security
- Data security

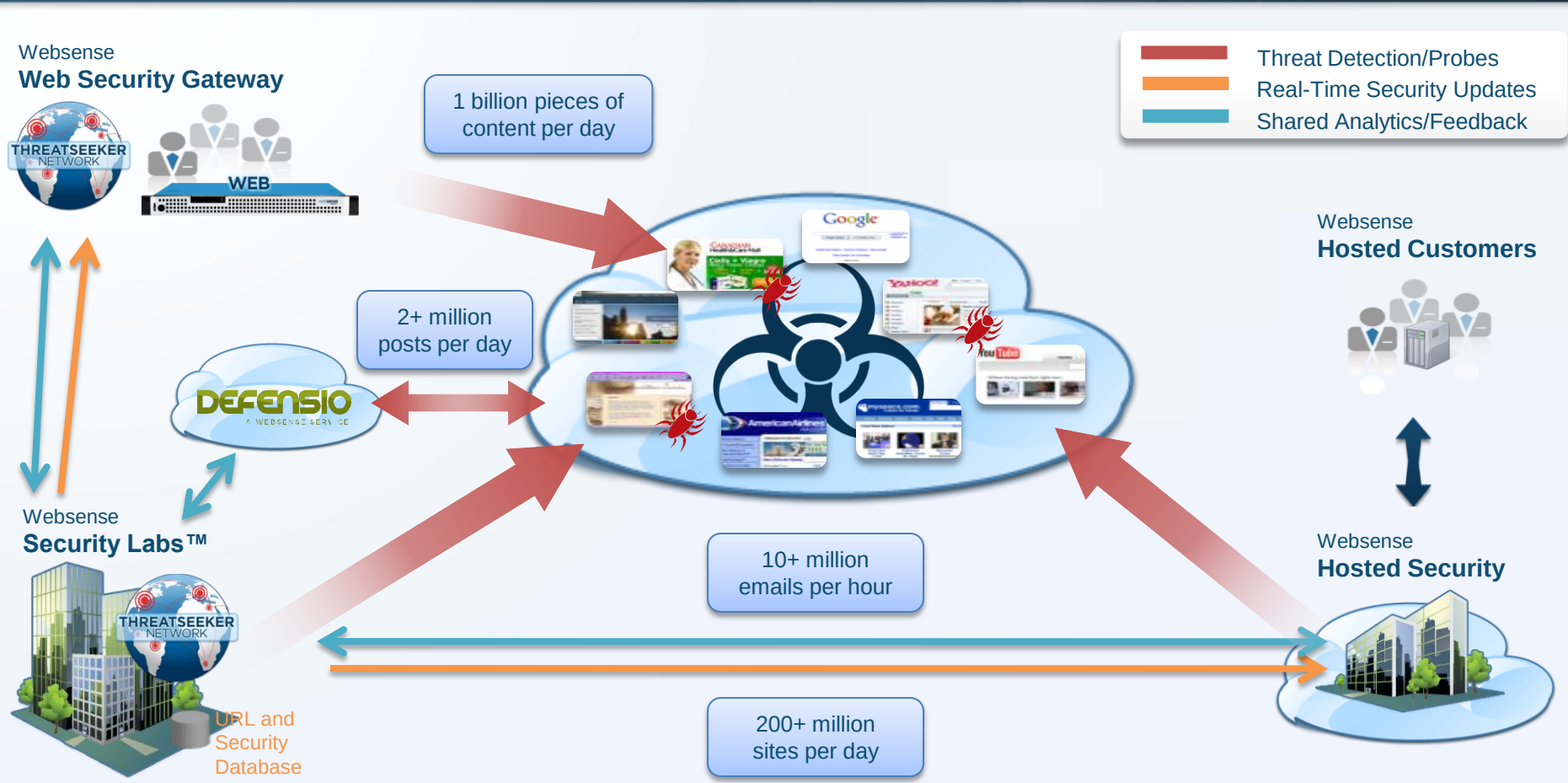
Solutions must be context-aware

websense®

- The technology needs to be context/content aware
  - Inbound traffic
  - Outbound traffic
  - Reputation
  - Data/Content classification
  - Anomalies
  - Protocol inspection

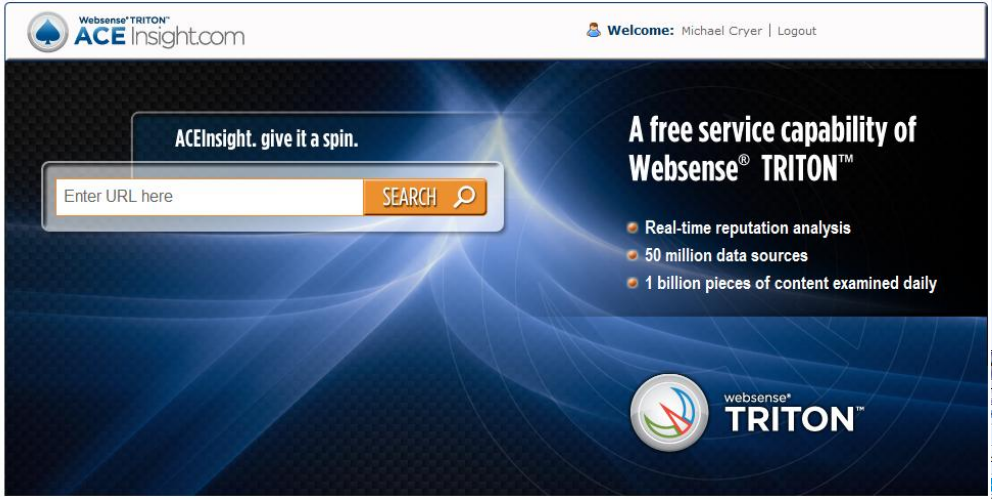
The ThreatSeeker Network

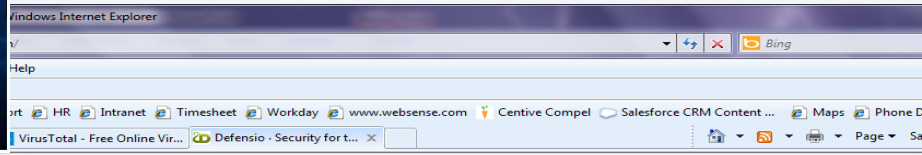
websense®



Free ThreatSeeker

websense®





ThreatSeeker Analytics

websense®

VIRUS TOTAL

Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this URL is benign. 0 VT Community user (s) with a total of 0 reputation credit(s) say(s) this URL is malicious.

Submission date: **2011-08-04 14:39:50 (UTC)**
Current status: **finished**
Antivirus report: View downloaded file analysis
Webscan result: **1/16 (6.2%)**

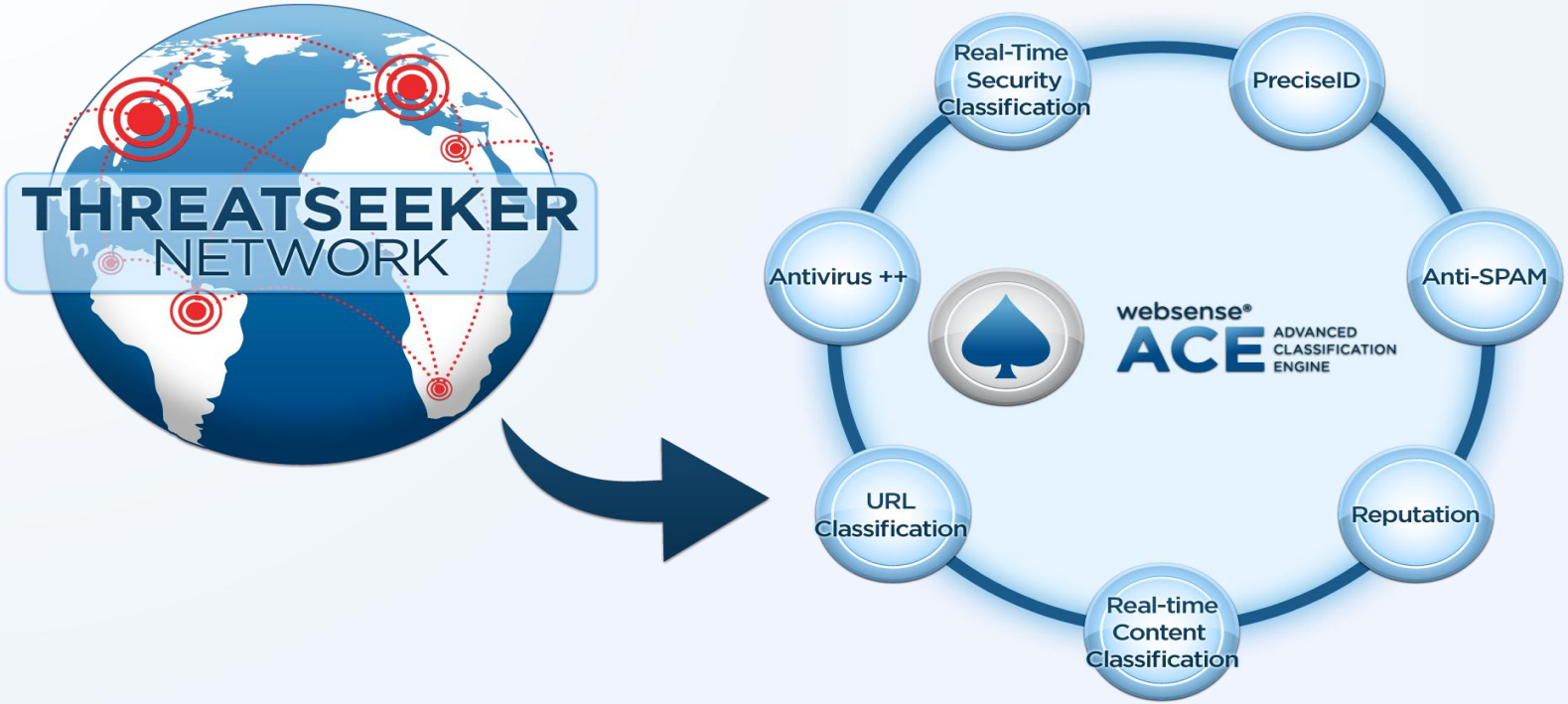
VT Community
not reviewed
Safety score: -

Compact | Print results

URL analysis tool	Result
Avira	Clean site
BitDefender	Clean site
G-Data	Clean site
MalcOde Database	Clean site
MalwareDomainList	Clean site
Opera	Clean site
ParetoLogic	Clean site
Phishtank	Clean site
TrendMicro	Clean site
Websense ThreatSeeker	Malware site
Wepawet	Error

Technology strategy

websense®



Technology strategy

- ACE allows us to protect customers where others do not
- Outbound content scanning is critical
- One analytic can trigger on its own or multiple engines can participate in voting algorithm
- Each analytic broken down in following slides

Technology strategy

websense®

- Real-time inspection and analysis of web content for the purpose of identifying exploit- and malicious code
- Built in parsing, obfuscation detection, de-obfuscation
- Specific attack ThreatID's, generic attack profiles, signatures, rules, attributes, kit detection, and anomalies
- Responsible for discovery of large zero-day attacks, including Aurora. Publicly cited by Microsoft on five of them

Technology strategy

websense®

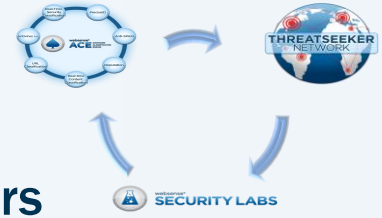
- Designed for known and unknown binary threats (executables)
- AV signatures for legacy and known attacks
- Integrated heuristics and signatures for unknown attacks
- Generic profiles and ThreatID's for kit created files and packers
- Inspection and advanced classification of exploitable file-types (PDF, SWF, Office files)

Technology strategy

- Designed as categorization filter, performance, and component of score
- 95+ categories (10 for security alone)
- 40+ updates per day
- Directly connects to cloud for additional lookups and attributes

Technology strategy

websense®



- Real-time content classifiers
- Machine learning classification (SVM+)
- Rules-based algorithms on URL and content
- Multi-lingual
- Special classifiers for large properties like Facebook
- Can be configured with weights and thresholds in the backend for accuracy vs. coverage and by customers

Technology strategy

websense®

- Designed for web and email, inbound and outbound
- 20+ points of reputation scoring (property, neighborhood, lexical, ASN, age, volume, anomalies, DNS, registration details, geography, etc)
- Real-time push of reputation updates
- Connects to cloud for additional feeds
- Scores generated in real-time and in backend

Technology strategy

websense®

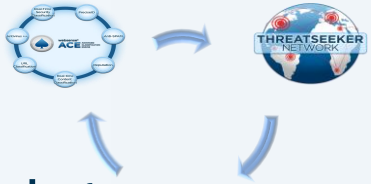
- Sender scoring and reputation
- Email message content scanning and scoring
- Heuristics
- Correlation over customer mails, scoring, volume, and type
- URL analysis and complete connections into other analytics

Technology strategy

websense®

- Designed for structured and unstructured data classification
- More than 800 shipping pattern policies
- More than 400 file-types support with parsing and decoding

Technology strategy - voting



- Voting or correlation is becoming more and more important with detecting complex and unknown threats.
- Simple example is real-time is unknown obfuscation type, site reputation is below score threshold, and URL DB is un-categorized = potential malicious site or sample.
- Complex example is URL is categorized as dynamic, reputation is questionable, content-type outbound is encrypted but not by SSL or a known encryption algorithm = potential APT / threat.

Prevention of Attacks – Email with Attachments

websense®

- The most prominent attack vector to gain access into organization is to blend threats together. Most usually start with an email to a target individual. The email either includes an attachment with an unknown exploit or a link to a website with a browser or file-based exploit. In most cases this email has context that is organization specific in order to provide authenticity and frequently is from another employee at the organization or is spoofed as one.

- Our Advanced Classification Engine will examine the email sending location, user, and content particulars to determine if there is suspect data there that matches. It is uncommon for modern malware to match any these characteristics in brand-new attacks, however we have seen common heuristics that may allow us to prevent here.

- Next we will do a deep analysis on the actual file that has been attached. This includes scanning through several Anti-Virus engines first. Again, it is rare that AV engines will have a signature match for an unknown file. At this point we have our own exploit analyses engine that will look into the file to determine if it has code, exploit attributes, or other anomalies. We often can catch code here that is suspect. One example is that it may be a PDF with embedded SWF actions or a Word DOC with a PDF with action script ,etc..

Prevention of Attack – Email with Links

websense®

Emails containing links to websites

- Often the content of the email is simply not sufficient to provide accurate classification in modern malware attacks. At this point our Advanced Classification Engine will examine the web URL to determine if it matches a security category and calculates the reputation of the destination site. At this point our engine will run through it's advanced exploit classifiers looking for known exploits, heuristics, and suspect content.
- In many cases of modern malware attacks not one of our classifiers has enough evidence to trigger an accurate classification. In this case we combine the net of all classifiers to determine a composite score. We call this concept voting. All engines participate in the scoring algorithm and different weights and thresholds are applied. This is the number one way we prevent modern malware attacks in phase 1 today.

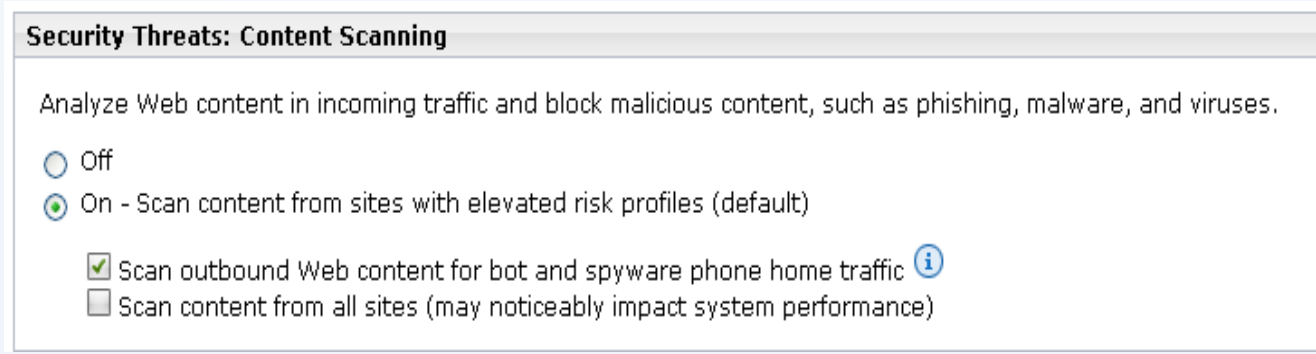
Dynamic DNS links contained in emails are very prevalent for these types of attacks.

Prevention of Attacks – Email with Links

websense®

Severing Command and Control

- Assuming that the attacker has successfully infected a host within the organizations network our defense then relies on the severing of the connections back to the command and control host. The most common ways that we have seen modern malware connect back is through the HTTP/HTTPs protocols, tunneling over port 80/443, or through a custom protocol. We recommend that customers do not allow custom protocol traffic to leave their networks. Because most do already we usually see the traffic going over open ports like 80 and 443.
- Triton Manager Outbound Scanning for Bot Traffic



Stopping the Attack

websense®

Outbound Command and Control Classification

- The Triton Architecture allows you to enable outbound inspection for the means of classifying and preventing command control connections post infection. When enabled all outbound traffic is inspect with the Advanced Classification Engine and assigned to policy.
- For Command and Control we will examine the destination, their reputation, the content, and the payload (if data), of the requests. Triton includes security categories that will match for outbound and sever the connection to the command and control host. The most common is the “bot network” category.
- Websense will release this month, the ability to block or control access to dynamic DNS sites for both web traffic and data loss prevention.

Outbound Protocol Inspection

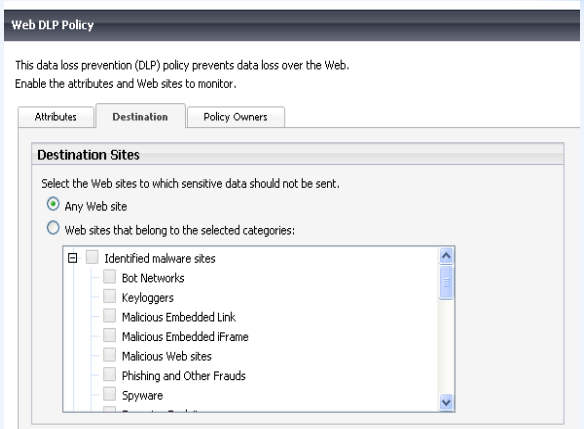
- Within the Web Security Gateway there is also the ability to inspect, examine, and classify content that traverses port 80 and 443. There are many cases when the command and control connection simply tunnel over port 80/443 but are not actually HTTP traffic. Here we have the ability not just to decrypt the traffic if it’s really HTTPS, but also to inspect the traffic for legitimacy, anomalies, and possible certificate exploitation.

Protecting the Data

websense®

Outbound Data Inspection

- Triton allows administrators to identify content that is unique to their environment that has intellectual property and other sensitive data in it. This can be done for a variety of supported document types, databases, and file formats. Our classification system is very accurate and contains representations of your data. With this we can identify data that has been modified without having to re-analyze it.



websense®

Questions?

Thank You...

TRITON™

- Web security
- Email security
- Data security