Cyber Security Experts

Newsletter **October 12, 2012**

EDEC Digital Forensics Releases Tarantula 2.0.

EDEC Digital Forensics, an innovator in the field of mobile forensics, has released Tarantula 2.0 beta which is a significant advance to affirm EDEC's position as the industry leader in Chinese phone forensics.

Tarantula 2.0 is an update of both Tarantula's hardware and software, including a new compact tip kit and USB-powered hardware unit as well as vastly improved analysis software that provides full file system analysis, acquires PIN codes and multiple IMEI numbers,

"Mobile forensic investigations are frequently done outside a lab environment. Our customers have been asking for these improvements from us and Tarantula 2.0 delivers," comments Mr. Judy, "Law enforcement, military and civilian examiners are often in the field, under difficult conditions, working to perform forensics or acquire intelligence on problematic devices."

Tarantula is the only forensic cell phone analysis system that supports physical extraction and decoding from all major Chinese manufactured chipsets — Mediatek, Spreadtrum, and Infineon, whether or not the phone is PIN-locked. Using full physical analysis, Tarantula 2.0 extracts and decodes low-level data including deleted data, decodes the phone file system and presents data such as call logs, SMS, phone book, media files, passwords, and IMEIs.

TOP VULNERABILITY THIS WEEK

The bank DDoS attacks being generated by the "itsoknoproblembro" script have continued apace over the last week, with rumors that defense contractors and others outside the banking industry are to be targeted soon.

As the attacks have worn on, additional details have come to light about the mechanisms being used, which are allowing potential targets to better protect themselves. Specifically, the script in question has been observed in the wild on compromised web servers with high-bandwidth links.

Business Leaders Urged to Step Up Response to Cyber Threats

Currently, too few company chief executives and chairs take a direct interest in protecting their businesses from cyber threats.

So now, for the first time, the Government and intelligence agencies are directly targeting the most senior levels in the UK's largest companies and providing them with advice on how to safeguard their most valuable assets, such as personal data, online services and intellectual property.

Today, the Government is launching a Cyber Security Guidance for Business at an event attended by FTSE 100 CEOs and Chairs, Ministers from Department for Business, Innovation and Skills, Foreign Office, Cabinet Office, Home Office and senior figures from the intelligence agencies.

Foreign Secretary William Hague, as Minister responsible for the Government Communications said:
"The UK is committed to building a secure, resilient, open and trusted internet. We are working with partners across the globe to ensure this vision becomes a reality.

"A networked world brings many advantages. But cyberspace – and cybercrime – knows no borders. Businesses must be alert to the dangers. Drawing on GCHQ's experience and working with industry the Government is committed to helping reduce vulnerability to attacks and ensure that the UK is the safest place in the world to do business."

Cyber Security Guidance for Business consists of three products:

1. The first products aimed at senior executives. It offer some high level questions which we believe will assist and support them to determine their critical information assets, support them in their strategic level risk discussions and help them ensure that they have the right safeguards and cultures in place.

2. The second product is an Executive Companion which discusses how Cyber Security is one of the biggest challenges that business and economy face today. It offers guidance for business on how together we can make the networks more resilient and protect key information assets against cyber threats. The document focuses around key points of risk management and corporate governance and includes some case studies based in real events.

3. The third product supports the Executive Companion and provides more detailed cyber security information and advice for 10 critical areas (covering both technical and process/cultural areas). If implemented as a set it can substantially reduce the cyber risk by helping to prevent or deter the majority of types of attacks. For each of these 10 areas, we have summarised the issue, outlined the potential risks and provided some practical measures and advice to reduce these risks. The material integrates the "Top 20 Critical Controls for Effective Cyber Defense". These controls provide further detailed guidance.

Mini Flame

Kaspersky Lab Discovers “miniFlame,” a New Malicious Program Designed for Highly Targeted Cyber Espionage Operations

Today Kaspersky Lab announced the discovery of miniFlame, a small and highly flexible malicious program designed to steal data and control infected systems during targeted cyber espionage operations.

miniFlame, also known as SPE, was found by Kaspersky Lab’s experts in July 2012, and was originally identified as a Flame module. However, in September 2012, Kaspersky Lab’s research team conducted an in-depth analysis of Flame’s command & control servers (C&C) and from the analysis found that the miniFlame module was actually an interoperable tool that could be used as an independent malicious program, or concurrently as plug-in for both the Flame and Gauss malware.

Analysis of miniFlame showed there were several versions created between 2010 and 2011, with some variants still being active in the wild. The analysis also revealed new evidence of the cooperation between the creators of Flame and Gauss, as both malicious programs can use miniFlame as a “plug-in” for their operations.

Main findings:

miniFlame, also known as SPE, is based on the same architectural platform as Flame. It can function as its own independent cyber espionage program or as a component inside both Flame and Gauss.

The cyber espionage tool operates as a backdoor designed for data theft and direct access to infected systems.

Development of miniFlame might have started as early as 2007 and continued until the end of 2011. Many variations are presumed to be created. To date, Kaspersky Lab has identified six of these variants, covering two major generations: 4.x and 5.x.

Unlike Flame or Gauss, which had high number of infections, the amount of infections for miniFlame is much smaller. According to Kaspersky Lab’s data, the number of infections is between 10-20 machines. The total number of infections worldwide is estimated at 50-60.

The number of infections combined with miniFlame’s info-stealing features and flexible

Continued…

Eugene Kaspersky: "Escalation of Cyber-Warfare is a Call for Action"

Eugene Kaspersky, CEO and co-founder of Kaspersky Lab, named international cooperation and advanced technology as the key requirements to survive the age of cyber-warfare. In his keynote speech at the ITU Telecom World 2012 conference, Eugene Kaspersky highlighted the dangers of the cyber-arms race and showcased Kaspersky Lab’s approach to protecting vulnerable industrial systems.

“In the long run, cyber-warfare is where all parties lose: attackers, victims and even uninvolved observers. Unlike traditional weapons, tools used in cyber-warfare are very easy to clone and reprogram by adversaries. The most important move to survive in this environment is the development and deployment of a new, advanced security paradigm for the most critical infrastructure.”

design indicate it was used for extremely targeted cyber-espionage operations, and was most likely deployed inside machines that were already infected by Flame or Gauss.

Discovery:

The discovery of miniFlame occurred during the in-depth analysis of the Flame and Gauss malware. In July 2012 Kaspersky Lab's experts identified an additional module of Gauss, codenamed "John" and found references to the same module in Flame's configuration files. The subsequent analysis of Flame's command and control servers, conducted in September 2012, helped to reveal that the newly discovered module was in fact a separate malicious program, although it can be used as a "plug-in" by both Gauss and Flame. miniFlame was codenamed SPE in the code of Flame's original C&C servers.

Kaspersky Lab discovered six different variations of miniFlame, all dating back to 2010-2011. At the same time, the analysis of miniFlame points to even earlier date when development of the malware was commenced – not later than 2007. miniFlame's ability to be used as a plug-in by either Flame or Gauss clearly connects the collaboration between the development teams of both Flame and Gauss. Since the connection between Flame and Stuxnet/Duqu has already been revealed, it can be concluded that all these advanced threats come from the same "cyber warfare" factory.

Name	Incidents (KL stats)	Incidents (approx.)
Stuxnet	> 100 000	> 300 000
Gauss	~ 2500	~10 000
Flame (FL)	~ 700	~5000-6000
Duqu	~20	~50-60
miniFlame (SPE)	~10-20	~50-60

Unlike Flame, the vast majority of incidents were recorded in Iran and Sudan, and unlike Gauss, which was mostly present in Lebanon; SPE does not have a clear geographical bias. However, we are inclined to believe that the choice of countries depends on the SPE variant. For example, the modification known as "4.50" is mostly found in Lebanon and Palestine. The other variants were found in other countries, such as Iran, Saudi Arabia and Qatar.

> "Learn the nuts and bolts of sophisticated fraud prevention"
>
> *Cyber Security Experts*

Functionality:

The original infection vector of miniFlame is yet to be determined. Given the confirmed relationship between miniFlame, Flame, and Gauss, miniFlame may be installed on machines already infected by Flame or Gauss. Once installed, miniFlame operates as a backdoor and enables the malware operators to obtain any file from an infected machine. Additional info-stealing capabilities include making screenshots of an infected computer while it's running a specific program or application in such as a web browser, Microsoft Office program, Adobe Reader, instant messenger service, or an FTP client. miniFlame uploads the stolen data by connecting to its C&C server (which may be unique, or "shared" with Flame's C&Cs). Separately, at the request from miniFlame's C&C operator, an additional data-stealing module can be sent to an infected system, which infects USB drives and uses them to store data that's collected from infected machines without an internet connection.

Alexander Gostev, Chief Security Expert, Kaspersky Lab, commented: "miniFlame is a high precision attack tool. Most likely it is a targeted cyberweapon used in what can be defined as the second wave of a cyberattack. First, Flame or Gauss are used to infect as many victims as possible to collect large quantities of information. After data is collected and reviewed, a potentially interesting victim is defined and identified, and miniFlame is installed in order to conduct more in-depth surveillance and cyber-espionage. The discovery of miniFlame also gives us additional evidence of the cooperation between the creators of the most notable malicious programs used for cyber warfare operations: Stuxnet, Duqu, Flame and Gauss."

US resist control of internet passing to UN agency

At present several non-profit US bodies oversee the net's technical specifications and domain name system.

They operate at arms-length from the US government but officially under the remit of its Department of Commerce.

There has been speculation that other nations will push for a change later this year, but they cannot force the US to comply.

The US has set out its position in documents filed with the International Telecommunications Union (ITU) - the UN agency responsible for encouraging the development of communications technologies.

The ITU is hosting a conference in December in Dubai to which representatives from 178 nations have been invited to review the International Telecommunications Regulations (ITR).

Close the gaps for cybercriminals

ThreatMetrix™ employs a range of techniques to gather details about a web transaction: from the device, the connection, and optionally shared transaction details. We then correlate this data with past transactions to identify anomalies, risk factors, and suspicious behavior.

Drawing upon hundreds of anonymous characteristics from a web transaction and analyzing them in real-time, ThreatMetrix reveals hidden truths about the device visiting your web site to help you decide whether to trust the computer to create a new account use a credit card or login.

TrustDefender™ ID extracts and uses the stores of static and dynamic data managed by browsers, operating systems, and TCP/IP packets to establish a unique identity and assess the risk in a web transaction in real-time.

TrustDefender™ Client identifies and isolates malware, verifies legitimate websites and protects online transactions with your site.

TrustDefender™ Cloud identifies transactions that have indicators of manipulation by malware or man-in-the browser (MitB) attacks.

The ThreatMetrix™ Cybercrime Defender Platform is the first industry solution that integrates sophisticated malware detection and advanced device identification technologies in a single, unified platform.

Most businesses deploy device identification and malware detection (if any) as separate solutions from different vendors. The insight uncovered resides in different silos, and doesn't deliver a common view of devices across systems. This makes it easier for cybercriminals to slip through the gaps in coverage. The overall strategy is inefficient, costly and incomplete.

The ThreatMetrix Cybercrime Defender Platform goes beyond combining malware detection and device identification – it supplements the combined solution with intelligence and analysis across the platform and throughout a global network of sites sharing fraud information.

By choosing an integrated solution, you gain the benefits of unified intelligence, simplified implementation and deployment, and better overall coverage. Most importantly, using integrated malware and device identification lets you protect the integrity of online transactions and identities

Threat Metrix ™

Cyber Security Experts

Information security issues—such as data breaches or employee misconduct—are a constant challenge for organizations, as they not only put sensitive data at risk, but can also cost your company time, revenue, and resources. No one is immune to data loss incidents—and no one is better equipped than CSE to help you identify and close gaps that put your organization's most important assets at risk.
At CSE, we know securing and managing electronically stored information (ESI) is critical to the future of your business. Our global team delivers scalable solutions to help you protect confidential and proprietary information from data security risks, such as malicious insiders, network vulnerabilities, and inadequate security policies.

Proven & Reliable Services

Coverage's:

- ✓ **Information Security Assessments**.
- ✓ Penetration Testing
- ✓ Policy Assessment & Design
- ✓ Data Breach Prevention

We have features for every step of the way.

Cyber Security Experts

P.O.Box 3928 Al-Khobar 31952
Kingdom of Saudi Arabia

info@cse-me.com

www.cse-me.com

cyber security
experts