

## Cyber Crime Threat Intelligence - Turkey

CSIS - Cyber Security Intelligence Service

Author – Stefan Frei, PhD

### Abstract

Cyber criminals effectively exploit the opportunities provided by the rise of the Internet and have, in just a few years, successfully stolen hundreds of millions of dollars from banks across the globe. The capability of cyber criminals to centrally control millions of compromised victims in botnets allows them to adapt quickly and launch new and targeted campaigns effectively. As prevention is limited, organizations are faced with the dilemma that they have to do business with a considerable share of infected clients, which calls for new approaches to combat these threats. CSIS operates a vast network of sensors to track botnet activity and cyber crime operations, and the data shows that emerging countries like Turkey are especially at risk. For example Turkey had 37 times more infections of the Sality botnet than Germany in 2014/Q1. Viable threat intelligence on cyber crime operations is key to identify infected machines in an organization, prevent the exfiltration of data, and to support multi-national efforts to disrupt botnets. This paper explains how cyber criminals operate botnets and compromise victims at large scale, and informs organizations how to best utilize cyber threat intelligence to protect their business and deal with infected customers. In today's threat environment, security is as much about prevention as it is about being prepared.

### Key Findings

- Emerging countries such as Brazil, South Korea, and Turkey are at increased risk for cyber crime attacks.
- Turkey has 37 times more *Sality* and 1.6 times more *Zeus Gameover* infections per 1,000 users than Germany, a country of similar population size but almost double the number of Internet users.
- Threat intelligence from botnets provides live insight into ongoing cyber crime campaigns, the population of infected users, and targeted organizations.
- CSIS recorded on average the addition of 4.3 new webinjects per day for the Zeus botnet in the last 12 months, targeting in total more than 2,000 identified organizations.
- It is not so much the absolute level of security that matters, it is about the difference. Cyber criminals exploit the weakest target first.

## Table Of Contents

<b>Abstract .....</b>	<b>1</b>
<b>Key Findings .....</b>	<b>1</b>
<b>1. Introduction .....</b>	<b>3</b>
<b>2. Know Your Enemy .....</b>	<b>4</b>
2.1. Attack Vectors .....	4
2.2. Controlling Targets / Botnets .....	5
<b>3. Threat Intelligence On Botnets .....</b>	<b>8</b>
3.1. Analysis of Botnet Configuration Files .....	8
3.2. Analysis of Infected Clients - Sinkholes.....	11
3.3. Why Attacking Turkey? .....	13
<b>4. Defense Measures .....</b>	<b>14</b>
<b>About CSIS Security Group .....</b>	<b>16</b>

## 1. Introduction

In the past decades we witnessed the increasing reliance of our society and economy on information technology and the Internet. Being fast adopters of new technology, criminals quickly found ways to exploit these new opportunities and have, in just a few years, successfully stolen hundreds of millions of dollars from banks across the globe, as reported by the FBI.<sup>1</sup> With a strong profit motive cyber criminals aggressively enhanced their malware tools to continuously stay well ahead of the latest advances in cyber security. This is a rapidly growing development. Malware innovations have been driven by attackers' goal to gain increasing control of compromised computer systems. Today's malware and cyber crime infrastructure is designed for the long-term control of millions of compromised machines ("botnets").

An advanced malware attack can no longer be seen as a single incident consisting of exploit, infection and remediation stages. Today's attacks are well coordinated efforts to infiltrate an organization or a large number of private users, and establish a foothold for the purposes of reconnaissance, exploitation, data exfiltration, and ongoing surveillance.

Advanced malware typically infects the victims web browser, allowing the malware to modify web pages and transactions in a completely covert fashion – undetectable on the backend of the targeted financial institution. Such malware allows criminals to bypass multifactor authentication and hijack fully authenticated sessions. Although multiple malware variants have been created, most are based on design and functionality principles of the Zeus Trojan – a highly polymorphic malware kit, capable of avoiding detection by most security technologies.<sup>2</sup>

The capability of botnets to centrally control and configure millions of compromised victims ("bots") further allows cyber criminals to adapt quickly and launch new and targeted campaigns effectively. Several recent reports and our own telemetry data on botnets indicate that emerging markets are especially at risk of compromise of privacy and data security. Brazil, South Korea, and Turkey are frequently identified as countries with the highest rate of compromise.<sup>3 4 5</sup>

In this paper we analyze CSIS threat intelligence data on two prevalent botnets, Zeus and Sality, focusing on financial fraud and infections in Turkey. We compare the cyber security state of Turkey with that of countries of the European Union.

Traditional approaches to security, like securing the perimeter and the back end, proved insufficient to combat these types of threats. Over time organizations have come to the realization that they have to do business with infected customers, whose infrastructure they can not control. This demands different approaches to security, information sharing, and threat intelligence.

---

<sup>1</sup> <http://www.justice.gov/opa/pr/2014/June/14-crm-584.html>

<sup>2</sup> <https://www.nsslabs.com/reports/online-banking-fraud-1-know-enemy>

<sup>3</sup> <http://www.infosecurity-magazine.com/view/38389/comment-mitigate-cyber-attacks-now-in-emerging-markets/>

<sup>4</sup> <http://www.infosecurity-magazine.com/view/36561/digital-access-leads-to-higher-malware-levels-in-developing-markets>

<sup>5</sup> [http://www.securelist.com/en/analysis/204792331/Financial\\_cyber\\_threats\\_in\\_2013\\_Part\\_2\\_malware](http://www.securelist.com/en/analysis/204792331/Financial_cyber_threats_in_2013_Part_2_malware)

Threat intelligence on cyber crime operations and botnets is key to identify infected machines in an organization, prevent the exfiltration of data, and to support multi-national efforts to disrupt botnets.

CSIS participated in the recent take-down of the Zeus botnet, a coordinated effort between the private industry and law enforcement, lead by the FBI. CSIS contributed with crucial telemetry data before and after the take-down for both Zeus and Cryptolocker, and provided detection and removal tools to eliminate this threat on infected machines.

## 2. Know Your Enemy

Understanding how modern malware works is a prerequisite to assess the risk and to develop an effective defense strategy and measures. In the last decade financial malware evolved from simple key loggers to advanced botnet platforms capable of defeating multifactor authentication, accompanied by sophisticated social engineering campaigns to trick unwary users into parting personally identifiable information (“PII”), which is then used in cross-channel fraud to further drain customer bank accounts.

Modern cyber crime campaigns are comprised of a multi-component system of *bots* and *command & control servers* to control the botnet. A bot depicts a compromised machine (in corporate or private use), command & control (“C&C”) servers are a key infrastructure component of botnets to allow cyber criminal the effective control of millions of bots.

The bigger a botnet, the more it can do because of its members’ compounded bandwidth and computing power. Besides hijacking user sessions, parts of a botnet can easily be rented out and retasked for distributed denial of service attacks (“DDoS”), spamming campaigns, distributed bitcoin mining, or password cracking.

### 2.1. Attack Vectors

The two primary attack vectors to infect and compromise a machine are *malware distribution* and *spear phishing*:

#### Malware Distribution

Cyber criminals either deploy exploit kits that poison search results, infect web advertisements or otherwise redirect users to the exploit kit, or they directly install exploit kits on hacked web sites. Once the user is redirected to the exploit kit, the users machine gets infected and the bot is installed. Typically, cyber criminals do not need 0-day attacks. A large number of systems worldwide still run the insecure Windows XP operating system, and/or many of the programs installed are not on the latest patch level. The market share of Windows XP in 2014/Q1 varies between 3.4 percent for Finland (with the lowest infection rates in

the EU) and 38 percent for Bosnia-Herzegovina. Turkey has a market share of Windows XP of 23.4 percent, well above the average in Europe of 16.4 percent.<sup>6</sup>

### Spear Phishing

In a spear phishing campaign cyber criminals use public sources such as LinkedIn, Xing, Facebook, company web sites, and business directories to gather information on likely targets. Using this information they send credible e-mails to the victims that purport to be from a trusted source, but actually contain droppers to install the malware.

### Evasion of Detection

To bypass malware detection engines cyber criminals automatically generate tens of thousands of unique permutations of the original malware, while retaining the core functionality of the malware. Thereafter each target is attacked with a unique sample of the malware. Cyber criminals further ensure their attacks go undetected by prior testing of malware samples against all anti-malware solutions on the market. Only samples not detected in these tests are then used for attack campaigns. This method continually proves to be very effective to bypass malware detection engines, and compromise systems at large scale.

### Post Infection

After successful infection of the target, the bot connects to the command & control server to upload the full information of the user and the specification of the infected machine. It then downloads and installs specific payloads and configuration information prepared by the fraudsters for the new target. This includes rules and functionality to disable locally installed anti-malware programs, and prevent the machine from accessing or getting updates from security sites. For most of the time the malware lies dormant until the user visits a web site specified in the bot configuration file – which then activates the attack and the hijacking of the user session, amongst other malicious activities. Thus, malware is designed to operate invisibly, making the identification and remediation of compromised systems an expensive endeavor – and results in extended times of compromise.

## 2.2. Controlling Targets / Botnets

Once a target is infected, the business objective of cyber criminals is to efficiently control a large number of distributed bots in a robust and reliable way while being resilient against takedown attempts – all in a way to prevent identification of the controlling bot master. A typical botnet infrastructure is shown in Figure 1, with the three principal components of a botnet, the *bot master*, the *command & control server*, and the *bot*.

---

<sup>6</sup> <http://gs.statcounter.com>

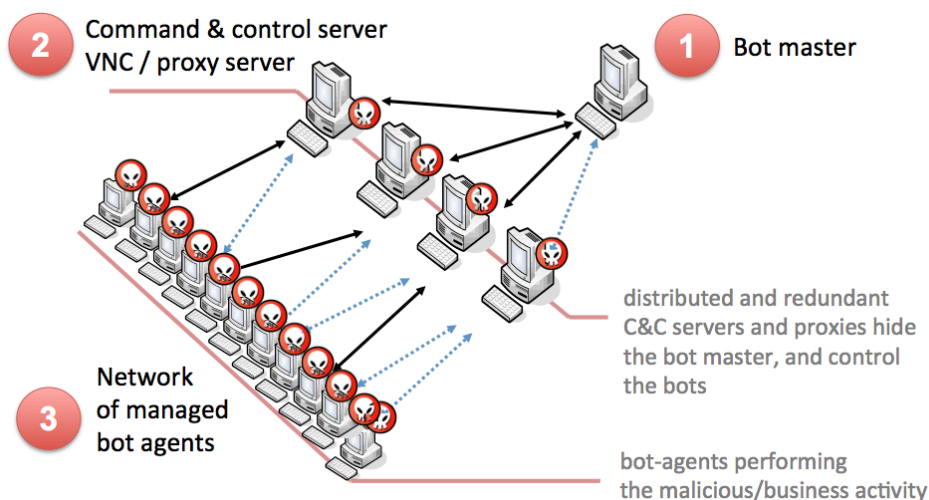


Figure 1 – Botnet overview

Bot Master	The bot master controls the network of compromised PCs through one or more intermediate layers of command & control servers. These layers of C&C servers effectively shield the bot master from detection and identification, and provide resiliency and redundancy to operate the bot net.
Command & Control Server	<p>A distributed and redundant set of compromised machines acting as command &amp; control servers. New instructions, payloads, and configurations prepared by the bot master are distributed to the bots through the C&amp;C servers.</p> <p>Key functions</p> <ul style="list-style-type: none"> <li>• Administrative and management panel for the bot master</li> <li>• Push updates to bots</li> <li>• Repository of data harvested by the bots</li> <li>• Act as proxy between bot and bot master</li> </ul>
Bot	<p>Software agent on the compromised victim machine. The bot renders remote control of the victim to C&amp;C server and runs the typical malicious activities, like key logging, disabling anti-malware programs, harvesting information.</p> <p>The bot activates whenever the user visits a specific site and implements hijacking of sessions (<i>webinjects</i>, defined later)</p>

### 2.2.1. Securing & Controlling The Botnet

Cyber criminals go at length to secure their control over the botnet against takedown attempts from law enforcement, the security community, or competing cyber crime gangs. To operate the botnet, the bot master has to address the following challenges:

- A. Anti-malware engines and security updates on the infected machine might disable and remove the bot.
- B. The communication between the bot and the C&C servers might be disabled or taken over by a third party resulting in the bot master losing control over his botnet.

Option (A) is a lesser issue for criminals as this approach implies to take action against the botnet on millions of globally distributed machines – a daunting task which does not scale well.

Securing the C&C infrastructure and communication channel of the botnet represents the true challenge to cyber criminals. Option (B) directly exploits the botnets single point-of-failure.

To control millions of bots in a robust manner cyber criminals operate an array of globally distributed command & control servers, hosted themselves on infected machines. This layer of C&C servers effectively shields the controlling bot master from identification, and provides resiliency against individually failing C&C servers. Cyber criminals therefore had to develop a robust method to allow a bot to identify a suitable C&C server, and switch to another C&C server if one is found unresponsive.

#### Domain Generation Algorithm

It is evident that bots can not rely upon a static list of preconfigured domain names or IP addresses that correspond to the location of the C&C servers, as these are easy to identify and blacklist.

Instead, cybercriminals have designed domain generation algorithms (“DGA”) that, given a particular date, time and seed value, will produce a large number of candidate domains.<sup>7</sup> The bot will then cycle through the list until it finds a “live” C&C server. The bot master, knowing the sequence of domains generated, only needs to register a few of these domain names to ensure control over the botnet.

The purpose of a domain generation algorithm is to:

- Make it impossible for static reputation systems to maintain an accurate list of all possible C&C domains.
- Maintain a small but agile physical C&C infrastructure that only needs to be configured and turned on for short periods of time.
- Provide the bot master “just-in-time” registration of domain names to avoid reactive counter-measures of law enforcement.

The large number of potential rendez-vous points (thousands of domain names generated per day) makes it difficult for law enforcement to effectively shut down botnets since infected computers will attempt to contact only some of these domain names every day to receive updates or commands.

---

<sup>7</sup> [https://www.damballa.com/downloads/r\\_pubs/WP\\_DGAs-in-the-Hands-of-Cyber-Criminals.pdf](https://www.damballa.com/downloads/r_pubs/WP_DGAs-in-the-Hands-of-Cyber-Criminals.pdf)

Further, all communication with the C&C servers is typically encrypted and signed, to prevent unauthorized parties to hijack the botnet after decoding the communication protocol in use.

### 3. Threat Intelligence On Botnets

Botnets are very interesting albeit difficult to fully analyze. The three main techniques to gather intelligence on ongoing botnet operations are *sinkholing*, *P2P crawling*, and *network traffic capturing*:

#### Sinkholing

Sinkholing is a technique that is used to redirect the traffic from bots to an analysis server. To identify and connect to the botnet's C&C servers, malware typically uses either hardcoded fail-over domains or a domain generation algorithm ("DGA") to generate possible rendez-vous points with one of the C&C servers. Reverse engineering of infected machines allows security researchers to identify and buy/register some of the rendez-vous domains, and thereby redirect all traffic of infected bots to the sinkhole server where intelligence is collected and analyzed once a bot uses one of these domains.

Knowledge of the domain names generated by the DGA's can be further used to protect organizations to identify infected machines, and prevent the bot from communicating with the botnet or exfiltrate data. For example, CSIS exposes the domain names generated by DGA's through their Secure DNS offering. Such services allow organizations to easily identify infected machines and prevent the exfiltration of data as the bot can no longer connect to the C&C server using these domain names.

#### P2P Crawling

Newer botnets have started to use a peer-to-peer C&C infrastructure. Based on the analysis of an infected machine it is possible to crawl each peer and thereby get insight into infected clients and the size of the botnet.

#### Network Capturing

Analyzing the network traffic of infected machines allows to determine and categorize the botnet.

CSIS practices all of the above techniques and operates an array of sinkholes which provide insight into millions of infected clients, the exfiltrated data, and ongoing cyber crime campaigns. Analysis and decrypting/decoding of botnet configuration files gathered in the process provides formidable insight into cyber crime campaigns and targets.

#### 3.1. Analysis of Botnet Configuration Files

The analysis of more than 4,000 botnet configuration files collected by CSIS in the last 12 months for different flavors of the Zeus malware provides a formidable insight on the targets and capabilities of cyber criminals.

The two main sections of configurations files are *domain blacklists* and *webinjects*:



### Domain Blacklist

In order to prevent the victim to automatically or manually update the machine and anti-malware solutions, the configuration file contains a list of domain names to be blocked. Figure 2 shows the top 20 of 4,606 blacklisted organizations with the number of sub level domains for each organization. The blacklists found in bot configurations are very exhaustive to ensure the bot is not exposed to any kind of security updates on the victims machine. As seen in Figure 2, the malware blocks access to all major security organizations and update services from software vendors to prevent the anti-malware programs and the software itself to receive updates. Using the C&C server infrastructure to push configuration files to infected clients allows cyber criminals to quickly update the blacklist and counter new threats.

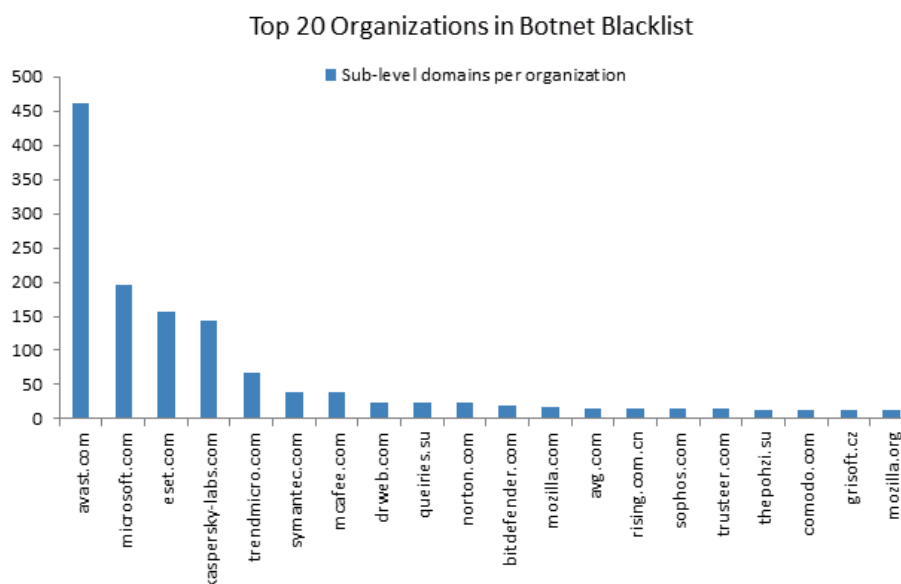
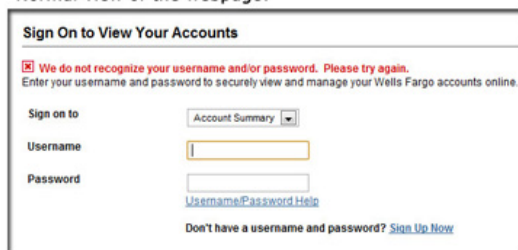


Figure 2 – Top 20 of 4,606 organizations blacklisted (and disabled) in botnet configuration files

### Webinjects

The bot configuration also contains a list of domain names of interest, together with *webinjects*. A *webinject* is the HTML code to be injected into the victims browser session in order to exfiltrate authentication data or insert fraudulent transactions. Figure 3 shows a *webinject* that hijacks the victims login credentials of the targeted site.

Normal view of the webpage:



The webpage injected with form fields:

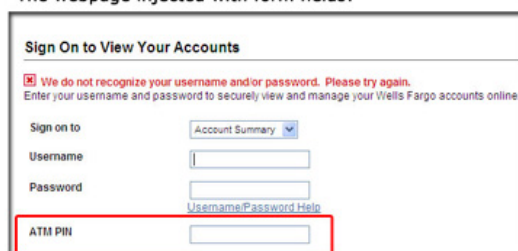


Figure 3 – Screenshot of clean site vs. site with *webinject* used to exfiltrate authentication data. Source (8)

If the bot master has interest in a particular site, he may also prefix the domain with the “@” parameter in the configuration file to obtain a screen shot of the victim’s every mouse click on this site. Figure 4 shows the number of domain names of interest to cyber criminals as found in botnet configuration files. More than 2,000 *webinjects* identified (each needs to be individually crafted by the fraudsters) demonstrate the industry scale of cyber crime operations, as well as the breath of targeted organizations.

In Figure 4 *rules* indicate the number of web sites cyber criminals are interested in. For each website the rule triggers a specific action, like redirecting the user to an fake banking web site, take screenshots, and/or deploy a *webinject*.

A *webinject* is supplied for 88 percent of the domain names of interest. Financial institutions are the primary class of organizations targeted, covered by 26 percent of the *webinjects*. These numbers also demonstrate the broad interest of cyber criminals to hijack not only financial institutions. CSIS identified numerous *webinjects* for all major and local social media platforms (Google, Facebook, Twitter, ..), membership portals (Miles & More, Nordstrom Card, ..), airlines/transport (Airberlin, ..), internet provider (Verizon, Comcast, ..), e-commerce sites (Amazon, EBay, ..), and security vendors websites. E.g. one security vendor found in the target list sells software exploits. Over the past 12 months, CSIS recorded on average the inclusion of 4.3 new *webinjects* per day.

<sup>8</sup> <http://about-threats.trendmicro.com/us/webattack/87/Trend+Micro+Researchers+Uncover+SpyEye+Operation>

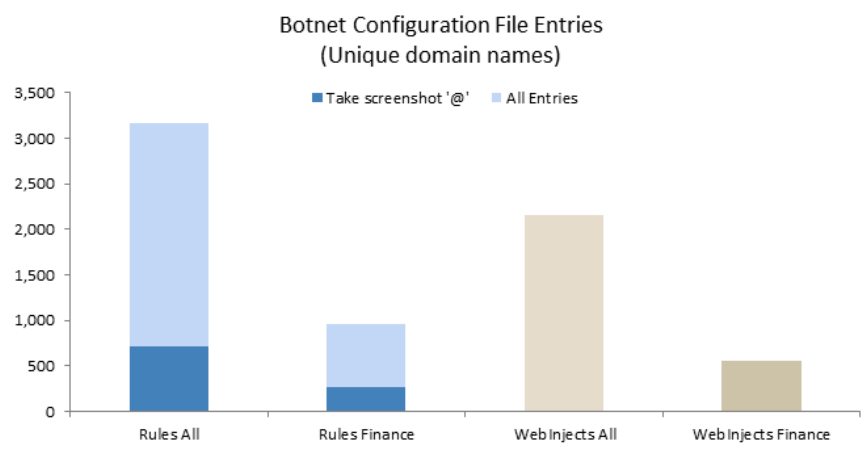


Figure 4 - Domain names of interest/to hijack by the bot

A detailed discussion and a sample of a decrypted botnet configuration file is documented in the threat report “*W32.Tinba (Tinybanker) The Turkish Incident*”.<sup>9</sup>

### 3.2. Analysis of Infected Clients - Sinkholes

In frequent intervals bots try to connect to the C&C server to exfiltrated data and receive new updates and instructions. If a C&C server domain points to a sinkhole, all the communication between the bot and the sinkhole server is recorded for analysis.

In the 90 days of 2014/Q1 6.6 million bot victims of the *Zeus Gameover* and *Sality* botnets connected to CSIS sinkholes from more than 200 countries worldwide. This is a representative sample of the victim population of the two botnets, but still a subset of the total size of just two botnets. For example, Figure 5 shows that between 1,000 and 1,500 Sality infected machines connected to CSIS sinkholes from Turkey every day in 2014 Q1.

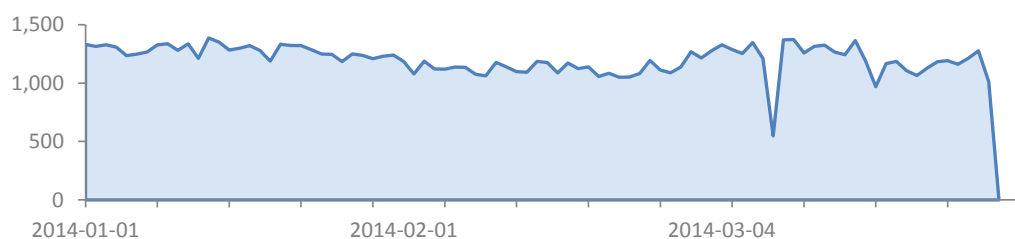


Figure 5 – Number of bots from Turkey connecting to CSIS sinkholes in 2014 Q1 (victims per day)

<sup>9</sup> [https://www.csis.dk/downloads/Tinba\\_White\\_Paper.pdf](https://www.csis.dk/downloads/Tinba_White_Paper.pdf)

Figure 6 compares the infection prevalence of the two botnets in Turkey with that of the 28 European Union (“EU”) member states to assess the geographical distribution of cyber crime campaigns. To compare infection rates, we measure for each country the number of infections per 1,000 users with internet access in 2014/Q1. The share of the population with internet access varies between 40% (Malta) to 96% (Denmark, Netherlands) in the EU, and 47% for Turkey.

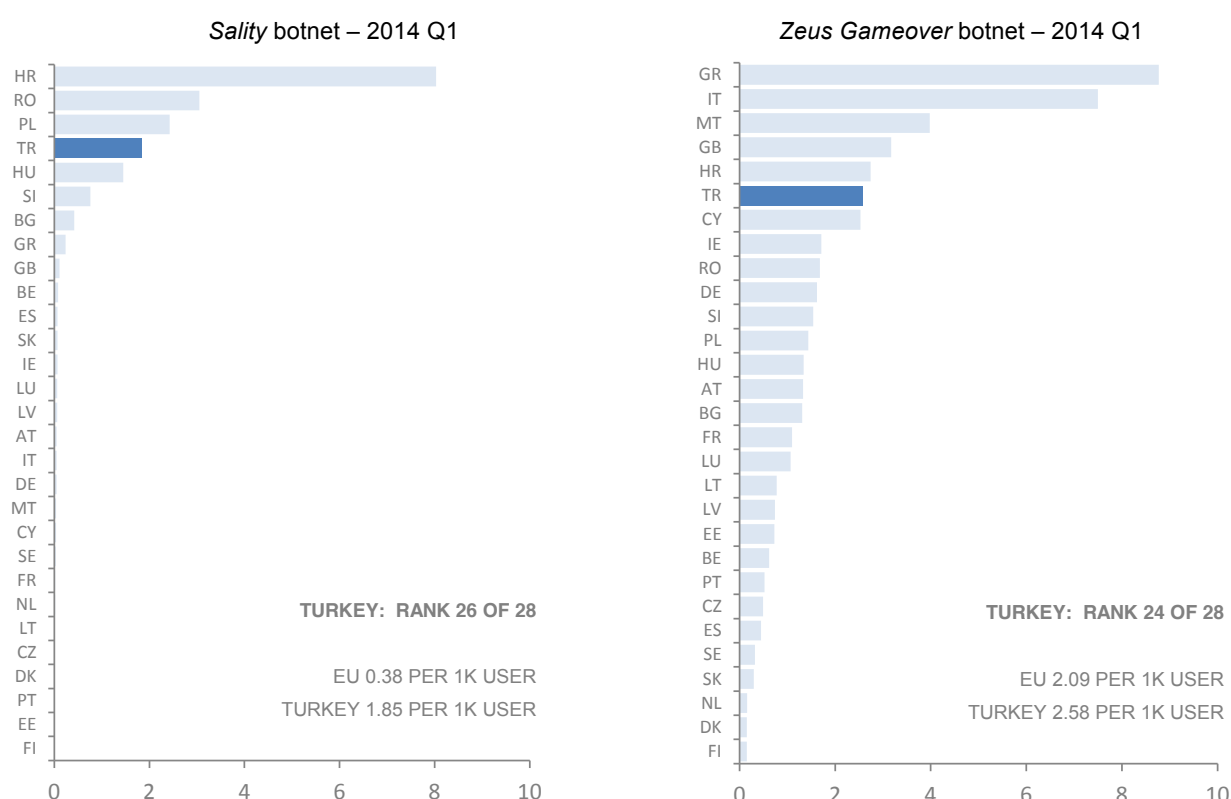


Figure 6 – Infections per 1,000 Internet users in EU and Turkey for 2014 Q1

Figure 6 shows a significantly skewed distribution of infections per 1,000 users amongst the EU and Turkey. This indicates a combination of poorer end-point protection, security preparedness of the population, and targeted cyber crime campaigns. Recent research identified a significant correlation between the rate of malware infections of a country and social, economic, and technological factors.<sup>10</sup>

For both botnets we found Turkey amongst the top most infected countries. For example, Turkey has 1.2 times more *Zeus Gameover* and 4.8 times more *Sality* infections per 1,000 internet users than the average of all EU countries.

<sup>10</sup> <http://download.microsoft.com/download/E/1/8/E18A8FBB-7BA6-48BD-97D2-9CD32A71B434/Cybersecurity-Risk-Paradox.pdf>

Figure 7 compares the population and infections rates of the two botnets between the EU, Germany, and Turkey. Germany has approximately the same population size as Turkey, but almost double the number of Internet users, yet Turkey shows considerably higher infections rates per 1,000 Internet users:

Turkey shows 37 times more Sality and 1.6 times more Zeus Gameover infections per 1,000 Internet users than Germany.

This is a clear indicator that Sality specifically targets Turkey (among a few other countries).

Metric	EU	Germany	Turkey
Population [million]	510.48	82.70	75.80
Internet User [million]	396.51	71.73	35.36
<b>Internet User [percent]</b>	<b>78%</b>	<b>87%</b>	<b>47%</b>
Market share Windows XP	N/A	11%	23%
<b>Sality Infections</b>			
Total	151,962	3,638	65,244
per 1,000 Internet users	0.38	0.05	1.85
<b>Zeus Gameover Infections</b>			
Total	829,895	116,101	91,286
per 1,000 Internet users	2.09	1.62	2.58
<b>Infections (both botnets)</b>			
Total	981,857	119,739	156,530
per 1,000 Internet users	2.47	1.67	4.43

Figure 7 - Botnet infections - Comparison between EU, Germany, Turkey for 2014/Q1

The vulnerable population in a given country is the same for both of the botnets compared. The considerable difference found between the infection rates between two botnets for Turkey supports the notion that cyber criminals specifically target regions of interest.

### 3.3. Why Attacking Turkey?

The CSIS data analyzed in this paper shows that cyber criminals have the infrastructure and operational capability to precisely target a specific country or organization. From a criminals perspective, given two valuable targets (e.g. two banks), it makes business sense to go after the weaker of the two targets. This approach is rewarded with the same or even a higher return as it is likely to successfully compromise more victims of the weaker target. Thus, emerging countries such as Turkey will continue to be specifically targeted as long as their security is not on par with that of comparable countries.

Typically, emerging countries have not yet achieved the security level and preparedness of developed countries, with respect of securing the population, end-points, and organizations. For example, Figure 7

shows that Turkey has more than twice the market share of the outdated and insecure Windows XP operating system when compared to Germany. Thus, the rapid economic growth of an emerging country (and with that the rise of revenue per target) makes them formidable targets for cyber criminals.

It all is about the difference of the security levels, not about the absolute level of security that dominates the target selection of the attacker. As long as a country or an organization has lower security compared to similar targets, it gets targeted more frequently and more intensely.

## 4. Defense Measures

Over the last years the industry has come to realize that *full protection or prevention* of cyber threats is an illusion. Cyber criminals continuously proved their ability to circumvent any kind of new defense measures introduced, and to quickly identify the weakest link in the security chain.

As banks moved to introduce SMS based authentication (for login and/or transaction verification) to counteract end-point based attacks, cyber criminals quickly adapted. Modules for mobile malware to overcome SMS based authentication were quickly deployed and are now available for all leading malware suites.

Typically, organizations have already implemented extensive backend protection and monitoring on their systems, paired with best practice controls from compliance frameworks. However, this still leaves the organization with the dilemma that it has to do business with a considerable share of infected clients (the infrastructure of which they do not control).

Organizations and governments have to perform a realistic risk assessment and threat management. A thorough understanding and monitoring of cyber criminals capabilities is essential to prepare against, and defeat modern attacks. Without viable threat intelligence on cyber crime operations, organizations focus on defending against known threats and will be taken by surprise of any kind of new security challenge, or breaches, which we learned to happen frequently.

To address these challenges:

- Enterprises must be prepared to do business with a large number of already compromised clients.
- Enterprises should assume their network is already compromised, and assume that it will continue to be compromised.
- As prevention is limited, enterprises should deploy tools and processes to quickly detect and remediate successful breaches, and detect compromised customers connecting to their systems.
- Enterprises should respond to a breach with a well a defined process rather than considering it to be an exception; have in place an incident response plan that is subject to routine review.

Organizations should therefore investigate the benefits of collaborating with industry partners to enhance real time threat intelligence for their continued risk assessment and antifraud efforts.

Third parties can provide threat intelligence to help detecting fraud and identify customers at risk. Customer-facing tools and services must be capable of informing risk management and anti-fraud tools that a customer has been compromised. Knowledge of current fraud schemes and campaigns will prove invaluable to prepare and/or alert customers at risk.

In todays threat environment, security is as much about prevention as it is about being prepared.

## About CSIS Security Group

CSIS Security Group is a privately held Danish IT security company originally founded in 1999.

### Values

CSIS Security Group operates with a set of values describing our way to act internally, towards our customers, as well as generally in the market. These values describe our culture and are the very framework for our decisions and strategies and thereby support us in all we do.

This set of values makes us capable of attracting and retaining some of the leading competencies within IT security. Our devoted staff and the company value set is the main reason why we keep strengthening our reputation as a trusted, loyal, and competent IT security advisor.

### CSIS Security Group product strategy

- CSIS Security group wants to offer the most extensive and cost effective IT security solutions for our customers. To reveal, document, and prevent security breaches for our customers. To support the IT security responsibly with gathering and analysis of information to prevent IT related crimes and harmful user behavior.
- CSIS Security Group IT security solutions ensure that management as well as the technical staff has access to an updated overview of the current status, and documents governance and control of security exposures 24x7.
- CSIS Security Group's target is to be among the top 3 suppliers within standardized, stabile, and modular IT security products, while providing economies of scale through a centralized solution with the possibility for strategic outsourcing

## Disclaimer

The information within this document may change without notice.

Use of this information constitutes acceptance for use in an "AS IS" condition.

There are NO warranties with regard to this information; CSIS Security Group has verified the data as thoroughly as possible.

In no event shall CSIS Security Group be liable for any consequences or damages, including direct, indirect, incidental, consequential, loss of business profits or special damages, arising out of or in connection with the use or spread of this information.

Any use of this information lies within the user's responsibility. All registered and unregistered trademarks represented in this document are the sole property of their respective owners.

The document may not be distributed or shared without prior written permission from CSIS Security Group A/S.