The Evolution of Cybercrime and Cyberdefense

Ed Cabrera, Robert McArdle, and the U.S. Secret Service
Criminal Investigation Division (CID)

A Joint Trend Micro and U.S. Secret Service Research Paper

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Cover image: Zhu Difeng | Shutterstock.com

Photo credits: Gonzales | Stephen Watt; Golubov, Vega, Horohorin, Kolarov, and Seleznev | U.S. Secret Service CID; Suvorov | www.amicusint.org; Tsastsin | Trend Micro FTR

All screenshots and diagrams in this paper were provided by the U.S. Secret Service CID and Trend Micro.

Contents

The Cradle of Cybercrime

The early years of the millennium was plagued by loosely interconnected networks of Russian-speaking cybercriminals intent on profiting from nefarious schemes. They raked in millions from trafficking in stolen payment card data to developing a robust underground network that provided bulletproof-hosting and online money laundering services. Over time, these networks produced and fielded the most innovative malware and botnets to prey on practically any individual or business online. Only in the past few years has the Russian underground's dominance begun to be challenged by various cybercrime hot spots.

A combination of factors could be responsible for the rise in organized online criminality in Russia. Some would argue that the country's emphasis on science, technology, engineering, and mathematics education in high school could be a reason why it has some of the most infamous hackers worldwide. While most advanced cybercriminals are very skilled or at least comfortable with computers and related technologies, advanced mathematics or engineering skills would certainly make for a very successful career in cybercrime. Others single out unemployment as the greatest contributor to the explosion of cybercrime.

In addition to harsh economic conditions, there are a few other reasons for the rise in cybercrime like lax law implementation. In the early 2000s, hardly any law enforcement agency or national legal system anywhere in the world was fully prepared for the legal and technical challenges posed by global organized cybercrime. This proved to be extra difficult for cash-strapped and resource-starved agencies in countries where cybercriminal underground markets thrived. To date, 72 percent of the countries across the globe have enacted cybercrime laws. Some agencies may not have the resources to pursue cases that do not directly lead to a suspect's home IP address, which meant any criminal who knows how to use VPN and proxy services or hire bulletproof-hosting companies may be able to evade responsibility for a crime.

Cybercriminals often target e-commerce, retail, and payment systems in North America and Western Europe because of the volume of valuable financial data that flows through them. Only a few, if any, of their victims physically reside in their home country and so domestic law enforcement agencies and prosecutors do not pursue and prosecute them.

A key component of for-profit criminality is getting paid for carrying out malicious activities. Cybercriminals have been known to abuse a reliable, ready-made, and largely unregulated payment infrastructure that used electronic currencies in years past (like WebMoney, Liberty Reserve, and Perfect Money) and today's cryptocurrencies (Litecoin, Bitcoin, and Monero). Though these currencies were not created for criminal use, they are preferred means of payment for illicit products sold and services rendered, as users were often asked no questions about the origin of their funds and transactions were left unrecorded.

A lot of transnational cybercrime in the late 1990s took place on Internet Relay Chat (IRC) channels, which proved to be raucous and disorganized as an e-commerce medium after some time. The cybercriminals behind early criminal networks like carder.org, carder.su, and CarderPlanet.com shifted to web-based bulletin board use. This gave the pioneer underground market a structure and its members a sense of discipline that allowed them to build their networks into online brands akin to major commercial service providers. Senior members further improved the underground economy by filling in roles like providing escrow services for illicit deals or vetting prospective vendors prior to membership.

Years later, underground marketplace, Silk Road, shone the spotlight on the Deep Web as an even better hiding place for criminals. The anonymity that Tor offered, pervasive use of cryptocurrency, and well-structured criminal outfits backed by a hierarchically organized staff all contributed to the continued growth and evolution of cybercrime. While it is impossible to provide a comprehensive history of cybercrime, we need to take at least a glance at its history and evolution to understand it.

2000-2010:
The Carding Era

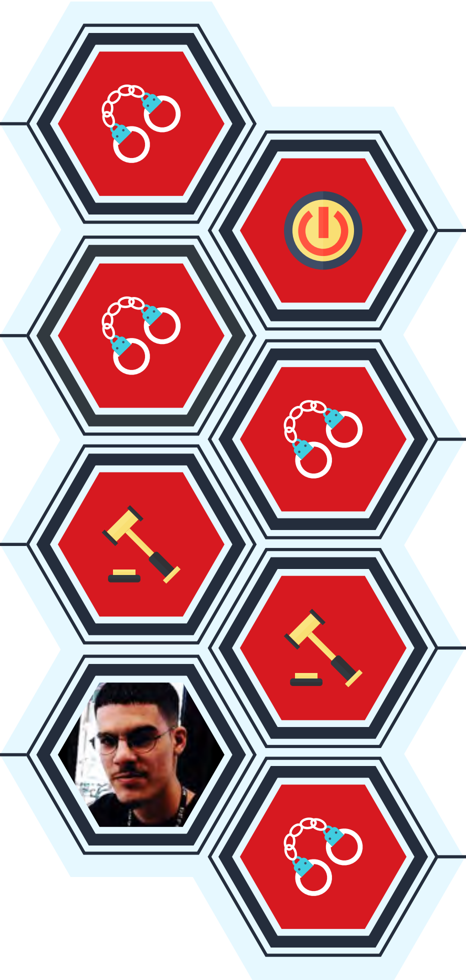
During what we dubbed the “carding era,” online and brick-and-mortar businesses, along with payment processing systems, were targeted by skilled hackers specifically looking for financial data. At the same time, payment card owners were subjected to phishing and intrusion attacks that gave cybercriminals unrestricted access to their personally identifiable information (PII). The stolen details were then sold to other criminals who could sell fake payment cards to customers. Probably the biggest and ultimately most influential of such underground sites was the CarderPlanet forum.

Today’s black-hat hackers or cybercriminals have come very far from the first hackers in the 1970s who stole long-distance telephone time from Bell, caused irregularities in the accounting data of the Lawrence Berkeley National Laboratory in 1986, or created the Morris worm shortly afterward. By 1990, FBI agents, through the U.S. Secret Service’s Operation Sundevil, already confiscated 42 computers and more than 20,000 floppy disks that were allegedly used for credit card and telephony service fraud. The cybercriminals of the 1990s were largely motivated by gaining notoriety and a thirst for uncensored information and knowledge.

Though the word “hack” in the context of computing owes its roots to the Massachusetts Institute of Technology as far back as 1955, use of the word spread to computer users in general in the 1960s. By 1963, “hacker” gained both its current white- and black-hat flavors.

Cybercriminals first gained much ground in former Soviet states, likely inspired by the huge profits that could be gained from what we now know as carding services. Underground forums and marketplaces in the countries soon sprang up and prospered. In carding forums and marketplaces, criminals sold lists of stolen payment card details to anyone who wished to carry out identity theft and payment card fraud for profit. Since then, carding and other criminal services have exponentially grown in both volume and scale.

The early 2000s was marred by threats that put computer users at the mercy of the beginnings of what would be the most notorious banking Trojans—ZeuS and SpyEye. Any individual or business who engaged in online financial transactions proved susceptible to the nefarious ploys that took root in the first criminal networks in the foremost underground market.



MARCH 2003

CarderPlanet don, Roman Vega, (aka Boa/Roman Stepanenko/ Randy Riolta/RioRita) was arrested in Cyprus and extradited to the U.S.

U.S. Secret Service

OCTOBER 2004

28 criminals involved in CarderPlanet and other similar networks were arrested (21 in the U.S. and 7 in 6 different countries)

U.S. Secret Service and partners

JULY 2005

CarderPlanet founder, Dmitry Golubov (aka Script), was arrested

Ukrainian Interior Ministry and the U.S. Secret Service

AUGUST 2007

Maksym Yastremsky (aka Maksik) was arrested in Turkey

U.S. Secret Service and Turkish authorities

JANUARY 2009

CarderPlanet don, Vega, pleaded guilty

U.S. Secret Service

MAY 2009

Aleksandr Suvorov pleaded guilty

U.S. Secret Service

25 MARCH 2010

Shadowcrew mastermind, Albert Gonzalez, was sentenced to 20 years in prison

U.S. Secret Service

27 AUGUST 2010

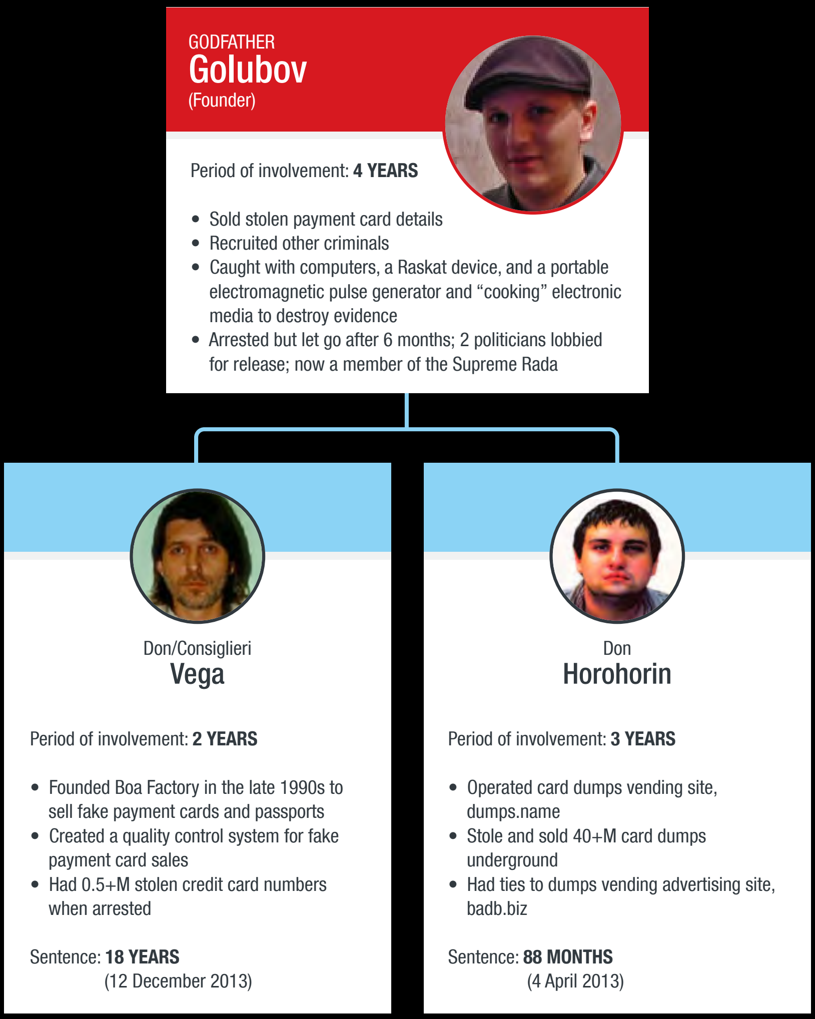
CarderPlanet don, Vladislav Horohorin (aka BadB), was arrested in France and extradited to the U.S.

U.S. Secret Service and French authorities

Figure 1: Cybersecurity wins from 2000 to 2010

Operation Firewall: The Path Toward CarderPlanet's Demise

CarderPlanet was founded in 2001 by Dmitry Golubov (aka Script). After some time, Roman Vega (aka Boa, Roman Stepanenko, Randy Riolta, or RioRita) and a number of other aspiring cybercriminals like Vladislav Horohorin (aka BadB) joined the organization. CarderPlanet had a mafia-like structure that was hierarchical in nature. It was led by a "Godfather" who was served by "Dons," "Capo di Capis," "Capos," and even an advisor known as the "Consigliere." The senior members of the organization were called "The Family" and used their authority to bring order and discipline to their criminal world.



GODFATHER
Golubov
(Founder)

Period of involvement: **4 YEARS**

- Sold stolen payment card details
- Recruited other criminals
- Caught with computers, a Raskat device, and a portable electromagnetic pulse generator and "cooking" electronic media to destroy evidence
- Arrested but let go after 6 months; 2 politicians lobbied for release; now a member of the Supreme Rada

Don/Consiglieri
Vega

Period of involvement: **2 YEARS**

- Founded Boa Factory in the late 1990s to sell fake payment cards and passports
- Created a quality control system for fake payment card sales
- Had 0.5+M stolen credit card numbers when arrested

Sentence: **18 YEARS**
(12 December 2013)

Don
Horohorin

Period of involvement: **3 YEARS**

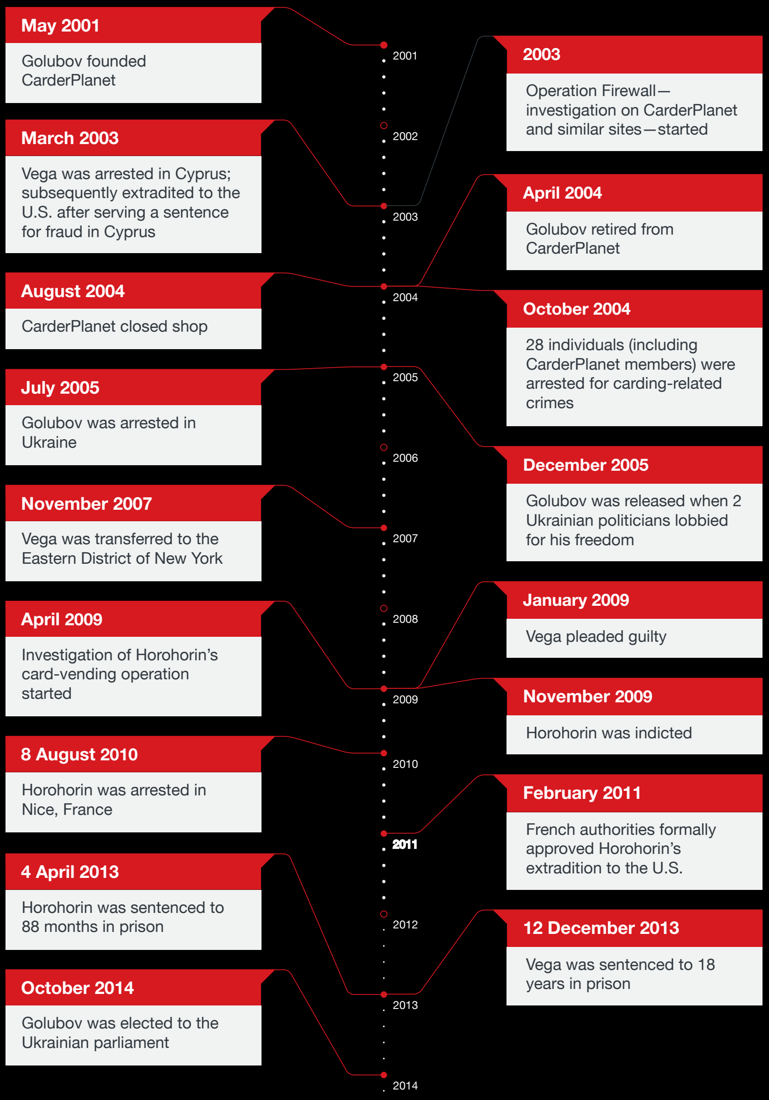
- Operated card dumps vending site, dumps.name
- Stole and sold 40+M card dumps underground
- Had ties to dumps vending advertising site, badb.biz

Sentence: **88 MONTHS**
(4 April 2013)

Figure 2: Profiles of CarderPlanet's early key members

CarderPlanet used electronic currencies like WebMoney for transactions. This practice provided buyers and sellers alike security and pseudo-anonymity, resulting in an "efficient and reliable online marketplace for stolen financial information akin to legitimate e-commerce sites." The site mostly used Russian though some posts were written in English.

When CarderPlanet closed shop in 2004, it had around 7,000 members. Some of its principal members were also believed to have ties with Shadowcrew, a notorious U.S.-founded clearinghouse for payment card fraudsters, and the RBS WorldPay gang. While most of the senior members of CarderPlanet spoke Russian, a smaller number of ranking members also communicated in English. Many of the latter were also active in the slightly smaller forum, Shadowcrew, which served as an online marketplace for stolen payment card data and other criminal goods and services.



May 2001
Golubov founded CarderPlanet

2003
Operation Firewall—investigation on CarderPlanet and similar sites—started

March 2003
Vega was arrested in Cyprus; subsequently extradited to the U.S. after serving a sentence for fraud in Cyprus

April 2004
Golubov retired from CarderPlanet

August 2004
CarderPlanet closed shop

October 2004
28 individuals (including CarderPlanet members) were arrested for carding-related crimes

July 2005
Golubov was arrested in Ukraine

December 2005
Golubov was released when 2 Ukrainian politicians lobbied for his freedom

November 2007
Vega was transferred to the Eastern District of New York

January 2009
Vega pleaded guilty

April 2009
Investigation of Horohorin's card-vending operation started

November 2009
Horohorin was indicted

8 August 2010
Horohorin was arrested in Nice, France

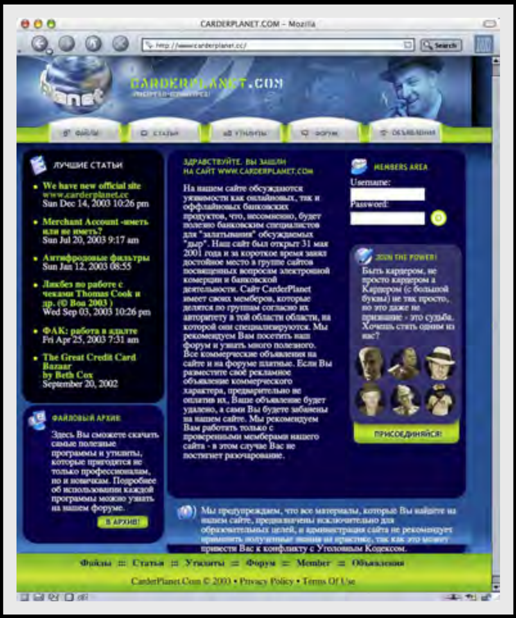
February 2011
French authorities formally approved Horohorin's extradition to the U.S.

4 April 2013
Horohorin was sentenced to 88 months in prison

12 December 2013
Vega was sentenced to 18 years in prison

October 2014
Golubov was elected to the Ukrainian parliament

Figure 3: Time line of investigation on CarderPlanet



CARDERPLANET.COM – Mozilla

http://www.carderplanet.cc/

ЛУЧШИЕ СТАТЬИ

- We have new official site www.carderplanet.cc Sun Dec 14, 2003 10:26 pm
- Merchant Account -иметь или не иметь? Sun Jul 20, 2003 9:17 am
- Антифродовые фильтры Sun Jan 12, 2003 08:55
- Ликбез по работе с чеками Thomas Cook и др. (© Boa 2003) Wed Sep 03, 2003 10:26 pm
- ФАК: работа в адалте Fri Apr 25, 2003 7:31 am
- The Great Credit Card Bazaar by Beth Cox September 20, 2002

ФАЙЛОВЫЙ АРХИВ

Здесь Вы сможете скачать самые полезные програмы и утилиты, которые пригодятся не только профессионалам, но и новичкам. Подробнее об использовании каждой програмы можно узнать на нашем форуме.

В АРХИВ!

ЗДРАВСТВУЙТЕ. ВЫ ЗАШЛИ НА САЙТ WWW.CARDERPLANET.COM

На нашем сайте обсуждаются уязвимости как онлайновых, так и оффлайновых банковских продуктов, что, несомненно, будет полезно банковским специалистов для "залатывания" обсуждаемых "дыр". Наш сайт был открыт 31 мая 2001 года и за короткое время занял достойное место в группе сайтов посвященных вопросам электронной комерции и банковской деятельности. Сайт CarderPlanet имеет своих мемберов, которые делятся по группам согласно их авторитету в той области области, на которой они специализируются. Мы рекомендуем Вам посетить наш форум и узнать много полезного. Все коммерческие объявления на сайте и на форуме платные. Если Вы разместите своё рекламное объявление коммерческого характера, предварительно не оплатив их, Ваше объявление будет удалено, а сами Вы будете забанены на нашем сайте. Мы рекомендуем Вам работать только с проверенными мемберами нашего сайта - в этом случае Вас не постигнет разочарование.

MEMBERS AREA

Username:

Password:

JOIN THE POWER!

Быть кардером, не просто кардером а Кардером (с большой буквы) не так просто, но это даже не призвание - это судьба. Хочешь стать одним из нас?

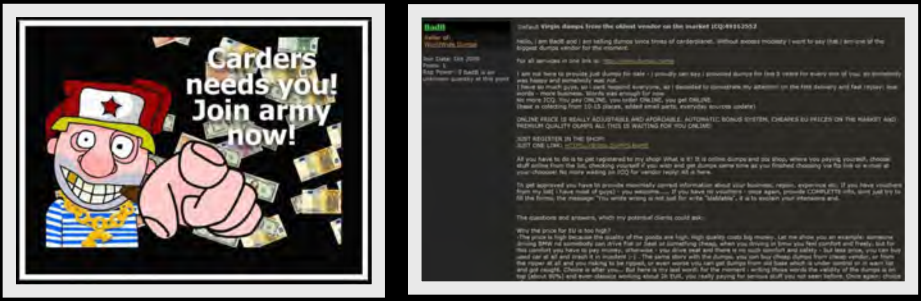
ПРИСОЕДИНЯЙСЯ!

Мы предупреждаем, что все материалы, которые Вы найдете на нашем сайте, предназначены исключительно для образовательных целей, и администрация сайта не рекомендует применять полученные знания на практике, так как это может привести Вас к конфликту с Уголовным Кодексом.

Файлы :: Статьи :: Утилиты :: Форум :: Member :: Объявления

CarderPlanet.Com © 2003 • Privacy Policy • Terms Of Use

Figure 4: CarderPlanet site before it was taken down



BadB

Seller of: WorldWide Dumps

Join Date: Oct 2009
Posts: 1
Rep Power: 0 BadB is an unknown quantity at this point

Default Virgin dumps from the oldest vendor on the market ICQ:[illegible]

Hello, I am BadB and I am selling dumps since times of carderplanet. Without excess modesty I want to say that I am one of the biggest dumps vendor for the moment.

For all services in one link is: [illegible]

I am not here to provide just dumps for sale - I proudly can say I provided dumps for last 8 years for every one of you, so somebody was happy and somebody was not.
I have so much guys, so I cant respond everyone, so I decided to concentrate my attention on the fast delivery and fast replays: less words - more business. Words was enough for now
No more ICQ. You pay ONLINE, you order ONLINE, you get ONLINE.
(base is colecting from 10-15 places, added small parts, everyday sources update)

ONLINE PRICE IS REALLY ADJUSTABLE AND AFORDABLE. AUTOMATIC BONUS SYSTEM, CHEAPES EU PRICES ON THE MARKET AND PREMIUM QUALITY DUMPS ALL THIS IS WAITING FOR YOU ONLINE!

JUST REGISTER IN THE SHOP!
JUST ONE LINK: [illegible]

All you have to do is to get registered to my shop! What is it? It is online dumps and cvv shop, where you paying yourself, choose stuff online from the list, checking yourself if you wish and get dumps same time as you finished choosing via ftp link or e-mail at your choose! No more waiting on ICQ for vendor reply! All is here.

To get approved you have to provide maximally correct information about your business, region, experince etc. If you have vouchers from my list(I have most of guys) - you welcome...... If you have no vouchers - once again, provide COMPLETE info, dont just try to fill the forms, the message "You wrote wrong is not just for write "blablabla", it is to explain your intensions and.

The questions and answers, which my potential clients could ask:

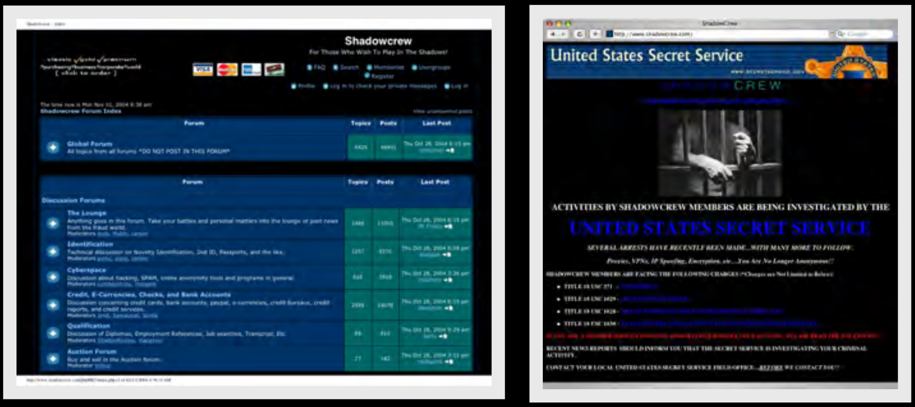
Why the price for EU is too high?
-The price is high because the quality of the goods are high. High quality costs big money. Let me show you an example: someone driving BMW nd somebody can drive fiat or Seat or something cheap, when you driving in bmw you feel comfort and freely, but for this comfort you have to pay money, otherwise - you drive seat and there is no such comfort and safety - but less price, you can buy used car at all and crash it in incedent :-). The same story with the dumps, you can buy cheap dumps from cheap vendor, or from the ripper at all and you risking to be ripped, or even worse you can get dumps from old base which is under control or in warn list and get caught. Choice is after you... But here is my last word: for the moment - writing these words the validity of the dumps is on top (about 90%) and even classics working about 2k EUR, you really paying for serious stuff you not seen before. Once again: choose

Figure 5: Proof of Horohorin's involvement in CarderPlanet

The U.S. Secret Service's Operation Firewall was one of the first major undercover operations targeting a criminal online carding organization. The operation's primary target was the largest English-language carding forum at the time—Shadowcrew—although many of its senior members were also active in similar sites like CarderPlanet, DarkProfits, StealthDivision, CVV.ru, and others.

Operation Firewall used a confidential informant, Albert Gonzalez, who had been arrested for ATM fraud in 2003. Gonzalez was well-known on CarderPlanet and Shadowcrew, which he helped revive along with Andrew Mantovani (aka Deck) and Anatoly Tyukanov (aka VoX or mengele). Gonzalez continued to work as a confidential informant following the Shadowcrew takedown in October 2004 although some of his behavior began to arouse suspicion. A separate criminal investigation revealed that Gonzalez had, during his off-hours, been involved in intrusions into the networks of several major U.S. retailers. Gonzalez was arrested in May 2008 in Miami, Florida, and was subsequently sentenced to two concurrent

20-year sentences for conspiracy; computer, wire, and access device fraud; and aggravated identity theft connected to the said intrusions.



Shadowcrew

For Those Who Wish To Play In The Shadows!

FAQ Search Memberlist Usergroups Register

Profile Log in to check your private messages Log in

The time now is Mon Nov 01, 2004 8:38 am

Shadowcrew Forum Index

Forum	Topics	Posts	Last Post
Global Forum All topics from all forums *DO NOT POST IN THIS FORUM*	[illegible]	[illegible]	Thu Oct 28, 2004 [illegible]

Forum	Topics	Posts	Last Post
Discussion Forums			
The Lounge Anything goes in this forum. Take your battles and personal matters into the lounge or post news from the fraud world. Moderators [illegible]	[illegible]	[illegible]	Thu Oct 28, 2004 [illegible]
Identification Technical discussion on Novelty Identification, 2nd ID, Passports, and the like. Moderators [illegible]	[illegible]	[illegible]	Thu Oct 28, 2004 [illegible]
Cyberspace Discussion about hacking, SPAM, online anonymity tools and programs in general. Moderators [illegible]	[illegible]	[illegible]	Thu Oct 28, 2004 [illegible]
Credit, E-Currencies, Checks, and Bank Accounts Discussion concerning credit cards, bank accounts, paypal, e-currencies, credit bureaus, credit reports, and credit services. Moderators [illegible]	[illegible]	[illegible]	Thu Oct 28, 2004 [illegible]
Qualification Discussion of Diplomas, Employment References, Job searches, Transcript, Etc. Moderators [illegible]	[illegible]	[illegible]	Thu Oct 28, 2004 [illegible]
Auction Forum Buy and sell in the Auction forum. Moderator [illegible]	27	142	Thu Oct 28, 2004 [illegible]

United States Secret Service

SHADOWCREW

ACTIVITIES BY SHADOWCREW MEMBERS ARE BEING INVESTIGATED BY THE

UNITED STATES SECRET SERVICE

SEVERAL ARRESTS HAVE RECENTLY BEEN MADE...WITH MANY MORE TO FOLLOW:

Proxies, VPNs, IP Spoofing, Encryption, etc....You Are No Longer Anonymous!!

SHADOWCREW MEMBERS ARE FACING THE FOLLOWING CHARGES (*Charges are Not Limited to Below):

- TITLE 18 USC 371 - [illegible]
- TITLE 18 USC 1029 - [illegible]
- TITLE 18 USC 1028 - [illegible]
- TITLE 18 USC 1030 - [illegible]

[illegible]

RECENT NEWS REPORTS SHOULD INFORM YOU THAT THE SECRET SERVICE IS INVESTIGATING YOUR CRIMINAL ACTIVITY.

CONTACT YOUR LOCAL UNITED STATES SECRET SERVICE FIELD OFFICE...BEFORE WE CONTACT YOU!!

Figure 6: Shadowcrew before (left) and after (right) Operation Firewall

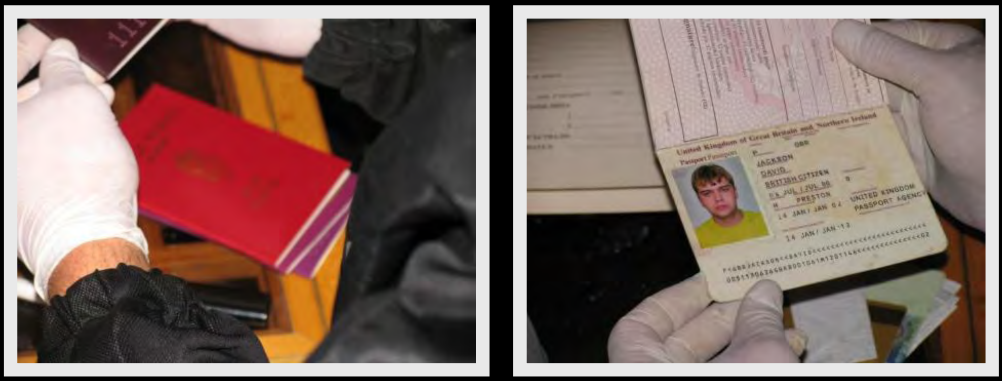

United Kingdom of Great Britain and Northern Ireland
Passport
UNITED KINGDOM PASSPORT AGENCY

Figure 7: Evidence seized via Operation Firewall

2011: Breaches Were Brought to the Fore

2011 was dubbed the "Year of Data Breaches," as the world witnessed organizations succumb to targeted breach attacks and lose what we have come to know as the new digital currency—information. The year was particularly challenging for the security industry, as several breached organizations soiled their reputations via the loss of confidential information and spent huge sums of money on fixing damages. Two of the biggest targets—RSA and Sony PlayStation—were left with no other choice but to publicly disclose facts about the attacks against their infrastructure so their customers could ensure proper mitigation.

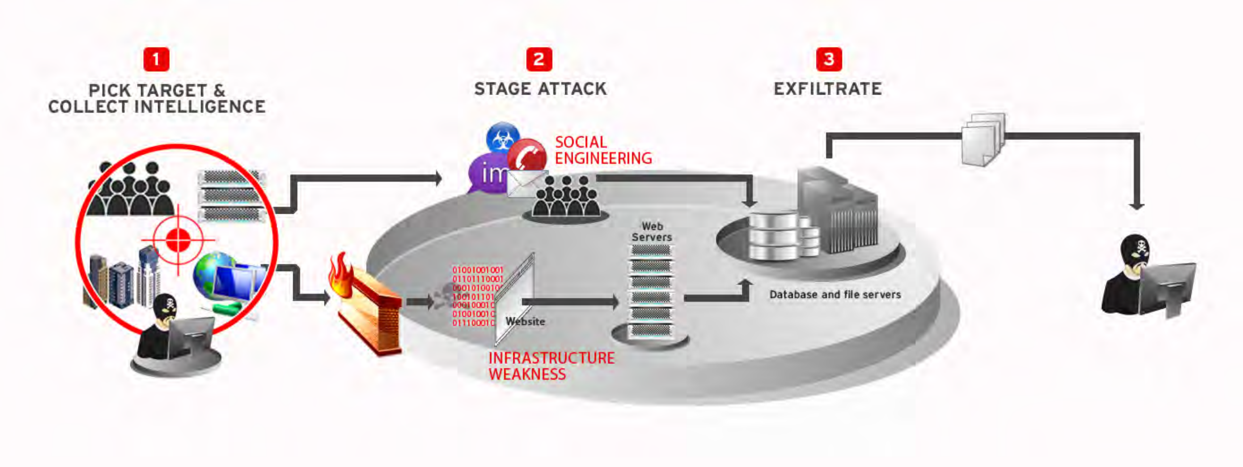


Figure 8: How data breach attacks work

The year was also plagued by mobile malware that sought to steal phone owners' personal data led by RuFraud and DroidDreamLight. Survey scams and all kinds of spam riding on trending topics littered social media sites, banking on reliable social engineering and hacking tactics and tools. On the vulnerability front, STUXNET-like DUQU could be considered one of 2011's nastiest system threats. Known data stealers, SpyEye, KOOBFACE, and FAKEAV, continued to figure in the threat landscape, along with multiplatform spam and malicious URLs. Hacktivist groups like Anonymous and LulzSec also kept on casting their dark shadows online with their own political agendas.

14 JUNE 2011

Operation Firewall: Shadowcrew criminal, Aleksey Kolarov (aka APK), was sentenced to 30 months in prison

U.S. Secret Service and partners

NOVEMBER 2011

Suvorov pleaded guilty to other charges

U.S. Secret Service

09 NOVEMBER 2011

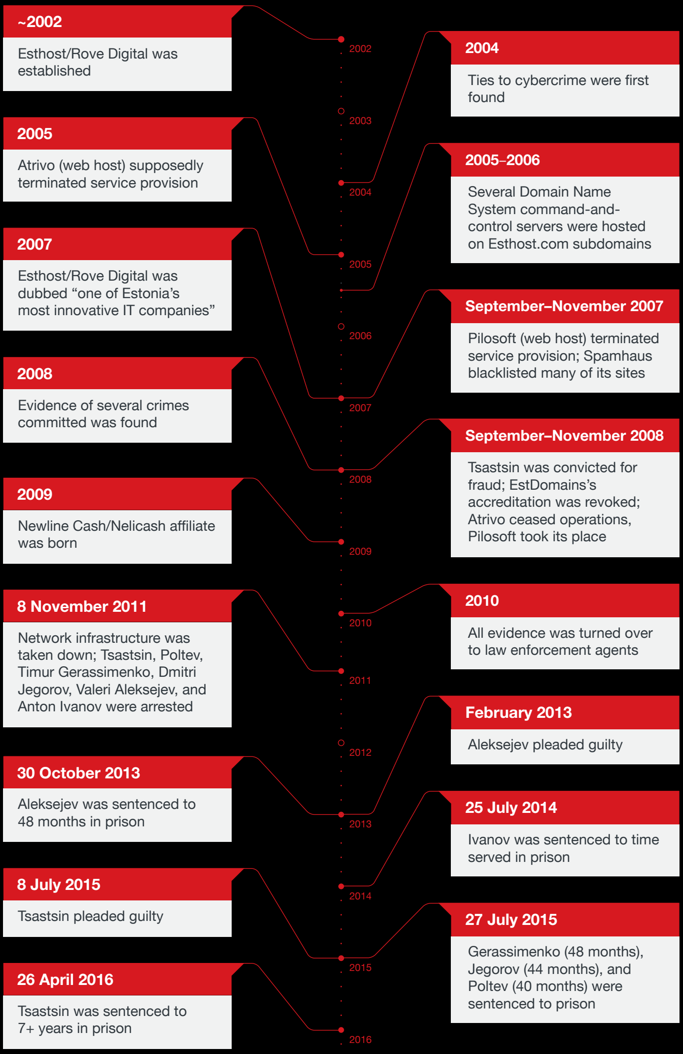
Operation Ghostclick: Esthost/Rove Digital was taken down; Vladimir Tsastsin and 5 other Estonian criminals were arrested

FBI with Trend Micro and other partners

Figure 9: Cybersecurity wins in 2011

Operation Ghostclick: The Esthost/Rove Digital Takedown

Esthost/Rove Digital was responsible for infecting approximately 4 million systems in more than 100 countries aided by advanced Trojans and large-scale click-fraud schemes, resulting in hundreds of millions of dollars' worth of damage and productivity loss for companies worldwide. The criminal network used several shell companies based in the U.S., Estonia, Ukraine, Denmark, and other countries for malicious activities; had an office in Tartu, Estonia; and was even touted as the "most innovative IT company" in the country in 2007 by a local newspaper.



~2002
Esthost/Rove Digital was established

2004
Ties to cybercrime were first found

2005
Atrivo (web host) supposedly terminated service provision

2005–2006
Several Domain Name System command-and-control servers were hosted on Esthost.com subdomains

2007
Esthost/Rove Digital was dubbed "one of Estonia's most innovative IT companies"

September–November 2007
Pilosoft (web host) terminated service provision; Spamhaus blacklisted many of its sites

2008
Evidence of several crimes committed was found

September–November 2008
Tsastsin was convicted for fraud; EstDomains's accreditation was revoked; Atrivo ceased operations, Pilosoft took its place

2009
Newline Cash/Nelicash affiliate was born

2010
All evidence was turned over to law enforcement agents

8 November 2011
Network infrastructure was taken down; Tsastsin, Poltev, Timur Gerassimenko, Dmitri Jegorov, Valeri Aleksejev, and Anton Ivanov were arrested

February 2013
Aleksejev pleaded guilty

30 October 2013
Aleksejev was sentenced to 48 months in prison

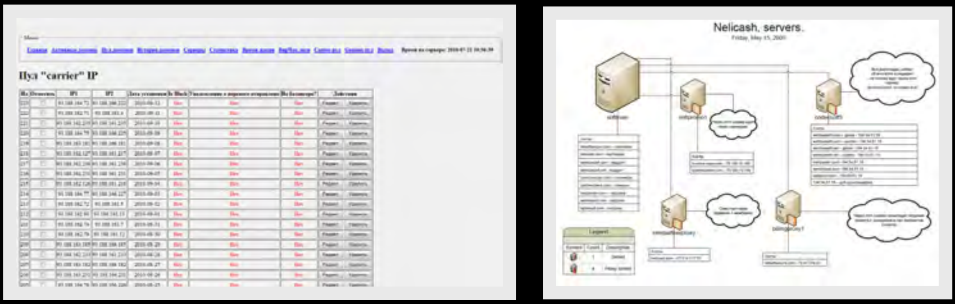
25 July 2014
Ivanov was sentenced to time served in prison

8 July 2015
Tsastsin pleaded guilty

27 July 2015
Gerassimenko (48 months), Jegorov (44 months), and Poltev (40 months) were sentenced to prison

26 April 2016
Tsastsin was sentenced to 7+ years in prison

Figure 10: Operation Ghostclick time line



Пул "carrier" IP

Figure 11: Evidence of Esthost/Rove Digital crimes

Esthost/Rove Digital infected around 500,000 systems in the U.S. alone, including those belonging to individuals, businesses, and government agencies like the National Aeronautics and Space Administration. The criminals manipulated internet advertising to generate at least US$14 million in illicit fees. In some cases, the malware used in attacks had the additional effect of preventing security software and OSs from updating, thus exposing infected machines to even more malicious software.

In the last few years prior to November 2011, Trend Micro researchers quietly worked with the FBI, the Office of the Inspector General, and security industry partners to take Esthost/Rove Digital down for good. This collaboration resulted in the successful seizure of the criminal network's infrastructure and arrest of major players, particularly CEO, Tsastsin, on 8 November 2011.

2012: The Post-PC Era

We declared 2012 the "post-PC era," as cybercriminals started moving away from previously favored targets to focus instead on attacking Android™, social media platforms, and even Macs. It took Android devices less than three years to reach the volume of threats (led by premium service abusers and data stealers) that it took 14 years for PCs to reach.

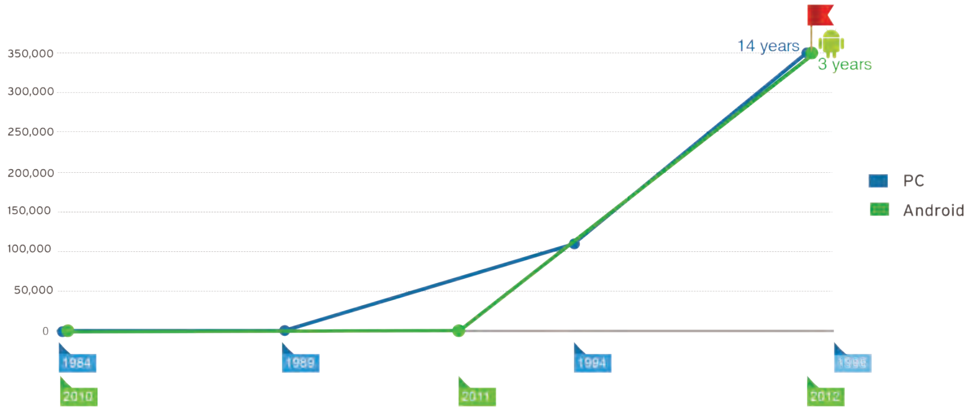


Figure 12: Android device versus PC threat volume growth comparison

In 2012, the question was no longer if a system would be breached but when, as data breach and targeted attacks became the new norms. Global Payments, the South Carolina Department of Revenue, and Zappos were among the top breach victims. Targeted attacks like LURID, Luckycat, Taidoor, and IXESHE, typically aided by spear-phishing emails, meanwhile, were among the most destructive threats. Readily available remote access Trojans like PoisonIvy, PlugX, Xtreme, JACKSBOT, and DRAT in underground markets also sped up the process of launching targeted attacks. More STUXNET-like malware like FLAMER (aka Mini-Flame) and GAUSS also surfaced as the year progressed.

Cybercriminals upped the ante in 2012 as well, as they fine-tuned their tools and tactics, most notably ransomware, automatic transfer systems, and the Blackhole Exploit Kit. Other threats also did not remain idle, as the volume of malware like ZeroAccess and VOBFUS significantly increased. Major underground market activity in Russia and China was also observed.

Figure 13: Cybersecurity wins in 2012

2013: Digital Bank Heists Dominated the Scene

Good old-fashioned stick-'em-up bank robberies were pushed to the curb by digital heists in 2013. Cybercriminals aided by sophisticated techniques to get hold of payment card numbers, bank accounts, and even PII in a matter of minutes took the place of traditional thieves. Information is, after all, the new currency. And with it on hand, cybercriminals can hold victims at their mercy, which should make us all realize that we stand to lose more than we think.

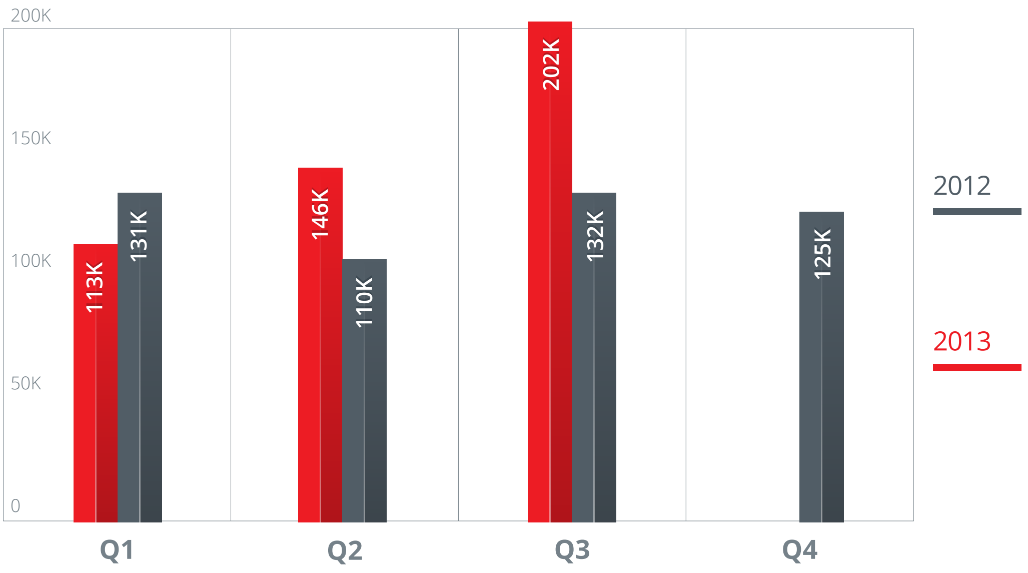


Figure 14: Comparison of online banking malware volume in 2012 and 2013

Throughout 2013, old threats were "refined." The online banking malware volume continued to increase even in countries they did not previously target as the year progressed. By October, the ransomware infection volume also rose, as the threat took on an even more crippling form in CryptoLocker. These and other refinements echoed what we predicted would happen—cybercriminals would improve their existing tools instead of create new ones.

The mobile malware volume surpassed the 1-million mark as early as September. And while media coverage on targeted attacks may have decreased, threat actors still went after chosen organizations in Brazil, France, and Germany. In the vulnerability space, Oracle's end of support for Java™ 6 led to problems that highlighted the risks involved with not upgrading or continuing to use unsupported software versions.

Taken together, while assaults against personal data were no longer new, they did not reach public consciousness as much as they did in 2013. Going after personal information proved to be a resounding theme highlighted by debates on Edward-Snowden-fueled revelations about state monitoring on citizens. 2013 may have, in fact, prompted everyone to ask one of the most important questions in today's digital age: "How can we keep our information safe?"

05 APRIL 2013

CarderPlanet don Horohorin, was sentenced to 88 months in prison

FBI and the U.S. Secret Service

03 MAY 2013

SpyEye criminal, Hamza Bendellaj (aka Bx1), was arrested in Thailand and extradited to the U.S.

FBI with Trend Micro and other partners

21 JUNE 2013

Trend Micro-INTERPOL partnership was forged

01 JULY 2013

SpyEye criminal, Aleksandr Panin (aka Gribodemon/Harderman), was arrested

FBI with Trend Micro and other partners

12 DECEMBER 2013

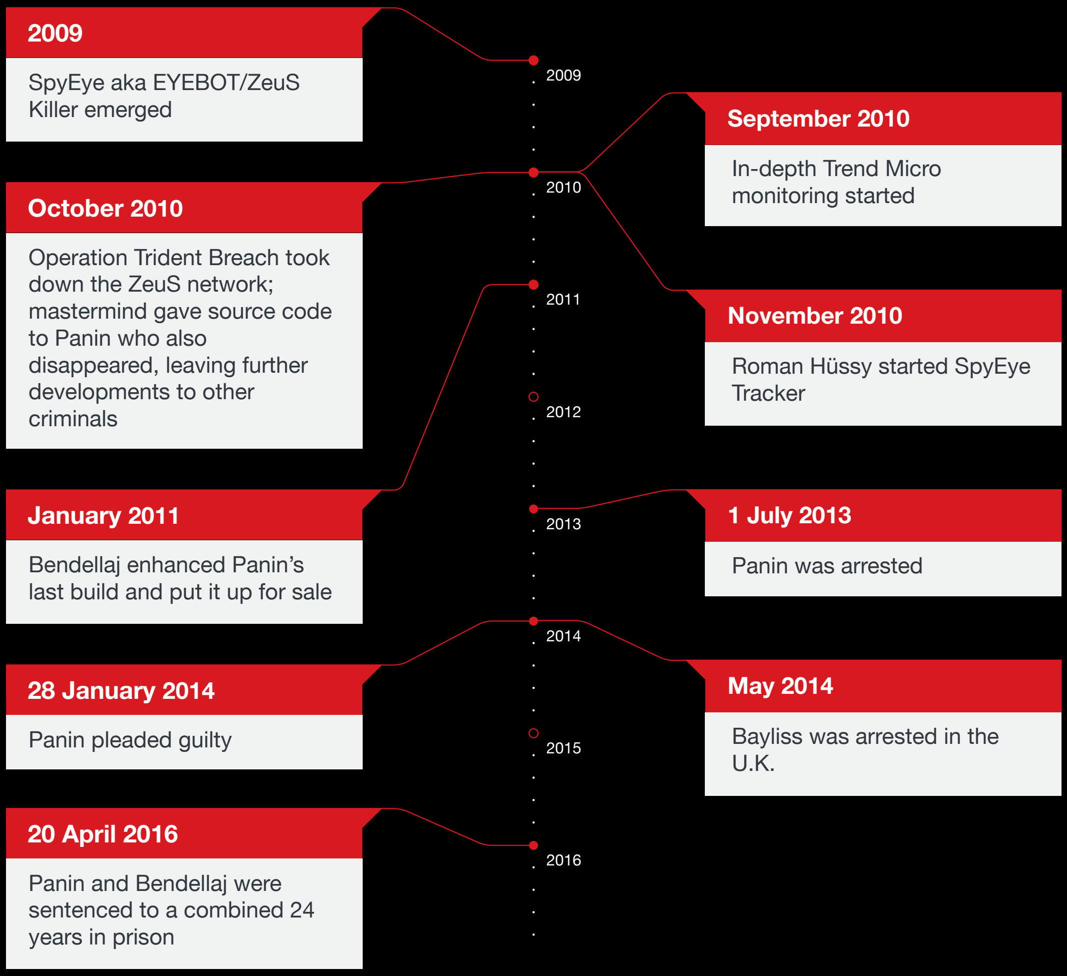
CarderPlanet don, Vega, was sentenced to 18 years in prison

U.S. Secret Service

Figure 15: Cybersecurity wins in 2013

The SpyEye Criminal Operation Takedown

SpyEye first made its way into the threat landscape as “ZeuS killer.” It was heralded as malware that could possibly take on ZeuS/ZBOT in a bot war. Like ZBOT, SpyEye was notorious for stealing user’s online banking and other financial credentials. It also has rootkit capabilities, which allowed it to hide processes and files from victims. When ZeuS’s author “Slavik” or “Monstr” left the cybercrime scene, he handed over his source code to SpyEye creator, Aleksandr Panin (aka Gribodemon or Harderman). Panin had other plans it seemed though, as he also disappeared from the cybercrime scene, leaving others to continue what he started. Hamza Bendellaj picked up where Panin left off. After years of investigation, both Panin and Bendellaj were arrested and later on incarcerated. Even known affiliates like James Bayliss (aka jam3s) did not escape the hands of the law.



2009

SpyEye aka EYEBOT/ZeuS Killer emerged

September 2010

In-depth Trend Micro monitoring started

October 2010

Operation Trident Breach took down the ZeuS network; mastermind gave source code to Panin who also disappeared, leaving further developments to other criminals

November 2010

Roman Hüssy started SpyEye Tracker

January 2011

Bendellaj enhanced Panin’s last build and put it up for sale

1 July 2013

Panin was arrested

28 January 2014

Panin pleaded guilty

May 2014

Bayliss was arrested in the U.K.

20 April 2016

Panin and Bendellaj were sentenced to a combined 24 years in prison

Figure 16: SpyEye case time line

2014: The Cyberattack Era

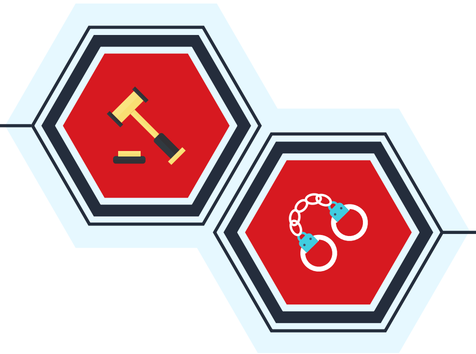
2014 showed just how destructive cyberattacks could be to individuals and companies alike. Effects of losing massive amounts of confidential data to attackers, substantive financial losses, and irreparable reputation damage ran rampant throughout the year. The severity of the cyberattacks we witnessed like those on Code Spaces, P.F. Chang's, Sony Pictures, Amtrak, and other companies and their effects revealed one thing—the risk of becoming the next victim definitely increased.

	WIPALL	STUXNET	BlackPOS	Master Boot Record Wiper in South Korea Attacks
Malware components	Several backdoors and malicious .SYS files	A worm, an .LNK file, and a rootkit	A Trojan	A dropper and a Trojan
Arrival/Autostart mechanism	Insufficient data	Arrives via USB drives;.LNK file executes copies of the worm	Exploits 4 vulnerabilities	Uses a link in spear-phishing emails; exploits a Hangul Word Processor vulnerability
Stealth mechanism	Disables a system's real-time scanner	Uses exploits and a rootkit component	Mimics security software to evade detection	Mimics legitimate Windows® services
Lateral movement	Uses predefined credentials to hack network shares	Installs client and server components to execute network commands	Insufficient data	Checks saved Secure Shell credentials for accounts with root access
Information stolen	Insufficient data	Allows attackers to view and alter project databases and information from the WinCC® server	Steals payment card credentials stored in infected point-of-sale (PoS) systems	Leaks confidential information
Purpose	File deletion from systems and fixed and remote drives	Control programmable logic controllers	Payment card data theft	Sabotage

Table 1: Proof of constant improvements to cybercrime and -attack tools

Breaches aided by PoS RAM scrapers showed a staggering increase in volume, making 2014 the "year of PoS malware" as well. Apart from massive-scale breaches, attacks targeting vulnerabilities like Heartbleed and Shellshock in widely used, previously considered secure open source software, along with FakeID and Same Origin Policy Bypass in mobile devices and platforms were also seen. Established processes like two-factor authentication also proved susceptible to attacks as shown by the criminals behind Operation Emmental.

Cybercriminals always set their sights on one thing—profit. They continued to indiscriminately hit data gold mines because peddling stolen information was lucrative as evidenced by the thriving cybercriminal underground economy.



29 JANUARY 2014

SpyEye criminal, Panin, pleaded guilty

FBI with Trend Micro and other partners

22 MAY 2014

SpyEye accomplice, James Bayliss (aka jam3s), was arrested in the U.K.

U.K. National Crime Agency (NCA) and Trend Micro

Figure 17: Cybersecurity wins in 2014

2015:
The Year of Big Botnet Busts

Shifts in the cyberthreat landscape aided by new technologies and attack models were seen in 2015. Familiar challenges became more complicated given changes in attackers' modus operandi. Data breaches did not just end with compromise; stolen information was instead leaked to the public or used in more damaging attacks like those on Ashley Madison members, Hacking Team, and the U.S. Office of Personnel Management.

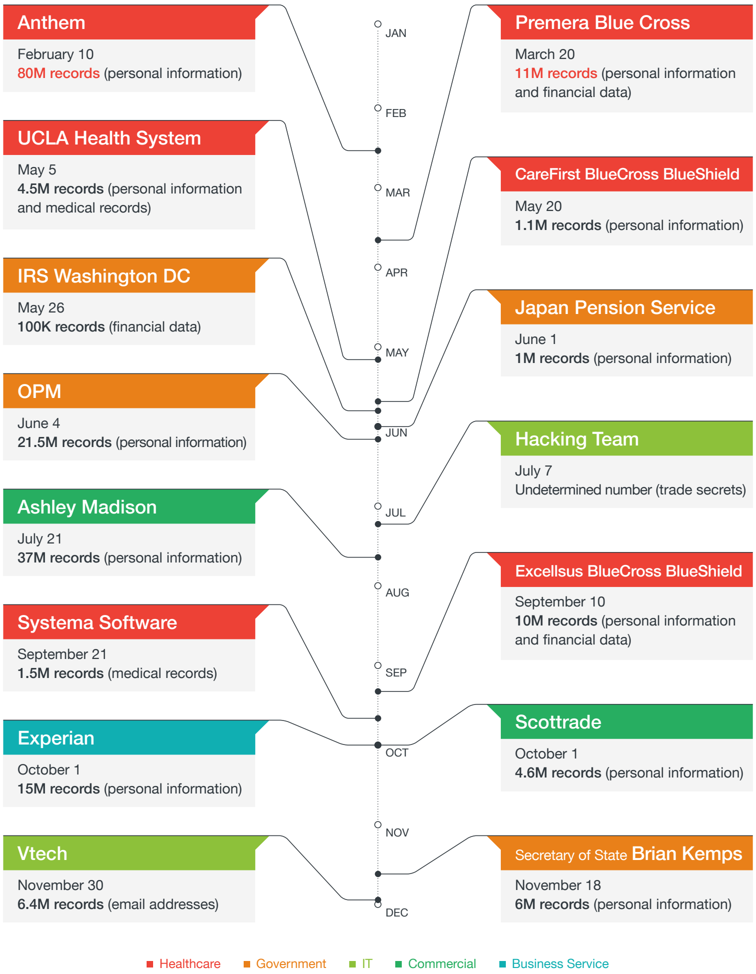
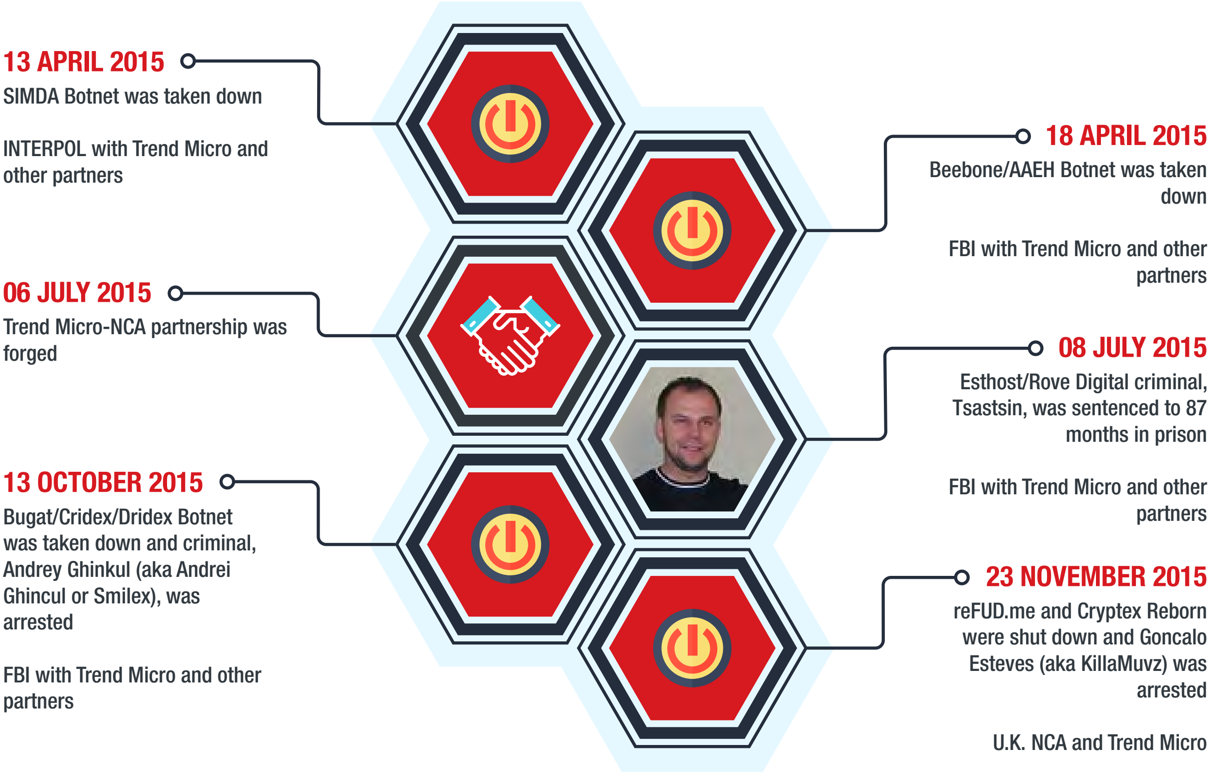

Anthem
February 10
80M records (personal information)
UCLA Health System
May 5
4.5M records (personal information and medical records)
IRS Washington DC
May 26
100K records (financial data)
OPM
June 4
21.5M records (personal information)
Ashley Madison
July 21
37M records (personal information)
Systema Software
September 21
1.5M records (medical records)
Experian
October 1
15M records (personal information)
Vtech
November 30
6.4M records (email addresses)
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
Premera Blue Cross
March 20
11M records (personal information and financial data)
CareFirst BlueCross BlueShield
May 20
1.1M records (personal information)
Japan Pension Service
June 1
1M records (personal information)
Hacking Team
July 7
Undetermined number (trade secrets)
Excellsus BlueCross BlueShield
September 10
10M records (personal information and financial data)
Scottrade
October 1
4.6M records (personal information)
Secretary of State Brian Kemps
November 18
6M records (personal information)
■ Healthcare
■ Government
■ IT
■ Commercial
■ Business Service

Figure 18: Biggest data breach attacks in 2015

Attacks that used zero-day exploits still prevailed, aided by advancements in exploit kits. These tools figured in cyberespionage campaigns like Pawn Storm. Crimeware offerings, portals, and training evolved to match cybercriminal demands in Brazil. Fledgling marketplaces emerged in France, Germany, Japan, and North America, alongside their more mature counterparts in Russia and China. All of these markets found ways to take advantage of darknets and the Deep Web.

Technological developments, particularly in the Internet of Things (IoT) space, also created a much broader attack surface. As the number of successful hacks on smart devices and vehicles grew, it was only a matter of time before threat actors found ways to exploit weaknesses for large-scale attacks, as our GasPot experiment showed.

Despite increased sophistication in threats and attacks seen in 2015 though, it was a great year for the good guys. The year was marked by several successful global takedowns and cybercriminal arrests. The takedown of long-standing botnets—Beebone/AAEH, SIMDA, and Bugat/Cridex/Dridex—and the arrest of major actors in criminal enterprises—Esthost/Rove Digital and reFUD.me—proved that cybercriminals were not above the law. Public-private partnerships (PPPs) between law enforcement agencies and security practitioners remained steadfast in keeping the world cybersecure.



13 APRIL 2015
SIMDA Botnet was taken down

INTERPOL with Trend Micro and other partners

18 APRIL 2015
Beebone/AAEH Botnet was taken down

FBI with Trend Micro and other partners

06 JULY 2015
Trend Micro-NCA partnership was forged

08 JULY 2015
Esthost/Rove Digital criminal, Tsastsin, was sentenced to 87 months in prison

FBI with Trend Micro and other partners

13 OCTOBER 2015
Bugat/Cridex/Dridex Botnet was taken down and criminal, Andrey Ghinkul (aka Andrei Ghincul or Smilex), was arrested

FBI with Trend Micro and other partners

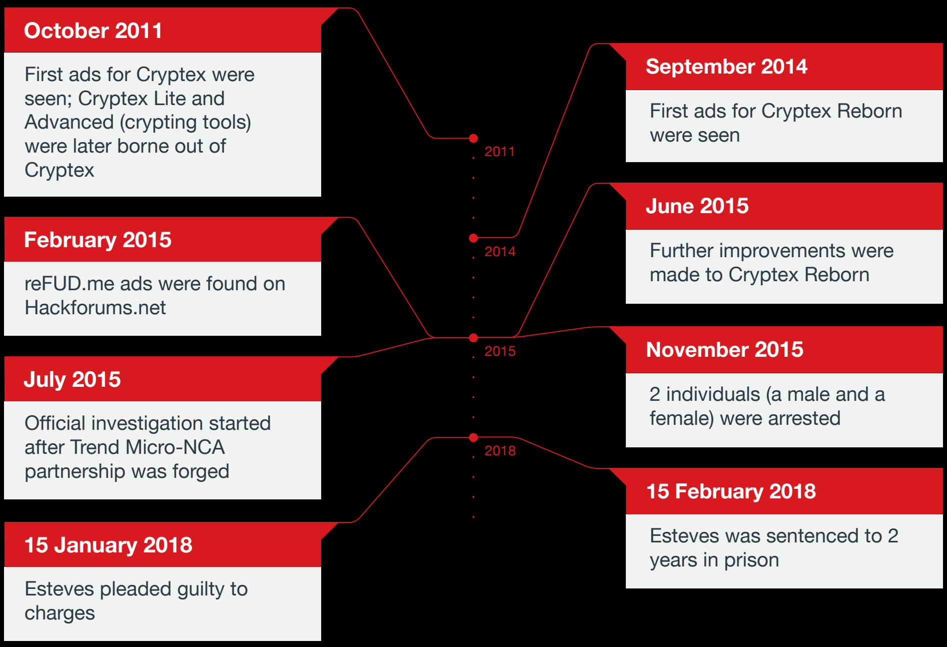
23 NOVEMBER 2015
reFUD.me and Cryptex Reborn were shut down and Goncalo Esteves (aka KillaMuvz) was arrested

U.K. NCA and Trend Micro

Figure 19: Cybersecurity wins in 2015

The reFUD.me/Cryptex Reborn Criminal Operation Takedown

The reFUD.me/Cryptex Reborn takedown on 23 November 2015 also led to the arrest and later incarceration of Goncalo Esteves (aka KillaMuvz). reFUD.me was heavily advertised in underground forums as early as February 2015. It was continually improved until at least June of the same year to bypass 30–40 of the best antivirus products in the market. Cryptex Reborn, meanwhile, was a popular crypting service that boasted of turning malware fully undetectable (FUD). After a couple of years of investigation, Esteves was sentenced to prison on 15 February 2018.



October 2011

First ads for Cryptex were seen; Cryptex Lite and Advanced (crypting tools) were later borne out of Cryptex

September 2014

First ads for Cryptex Reborn were seen

February 2015

reFUD.me ads were found on Hackforums.net

June 2015

Further improvements were made to Cryptex Reborn

July 2015

Official investigation started after Trend Micro-NCA partnership was forged

November 2015

2 individuals (a male and a female) were arrested

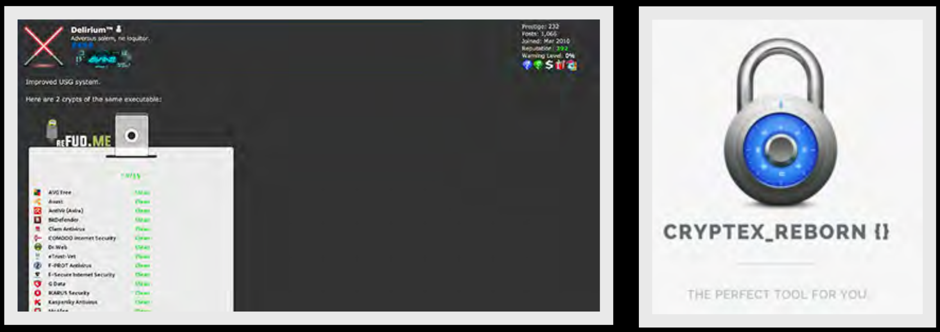
15 January 2018

Esteves pleaded guilty to charges

15 February 2018

Esteves was sentenced to 2 years in prison

Figure 20: reFUD.me/Cryptex Reborn case time line



Delirium™

Adversus solem, ne loquitor.

Prestige: 232
Posts: 1,066
Joined: Mar 2010
Reputation: 392
Warning Level: 0%

Improved USG system.

Here are 2 crypts of the same executable:

AVG Free	Clean
Avast	Clean
AntiVir (Avira)	Clean
BitDefender	Clean
Clam Antivirus	Clean
COMODO Internet Security	Clean
Dr.Web	Clean
eTrust-Vet	Clean
F-PROT Antivirus	Clean
F-Secure Internet Security	Clean
G Data	Clean
IKARUS Security	Clean
Kaspersky Antivirus	Clean
McAfee	Clean

Figure 21: Evidence gathered on reFUD.me/Cryptex Reborn

2016:
The Digital Extortion Era

2016 was a trying year for enterprises, as cyberthreats caused billions of dollars in corporate losses. It was indeed the "year of online extortion" with ransomware and business email compromise (BEC) leading the charge.

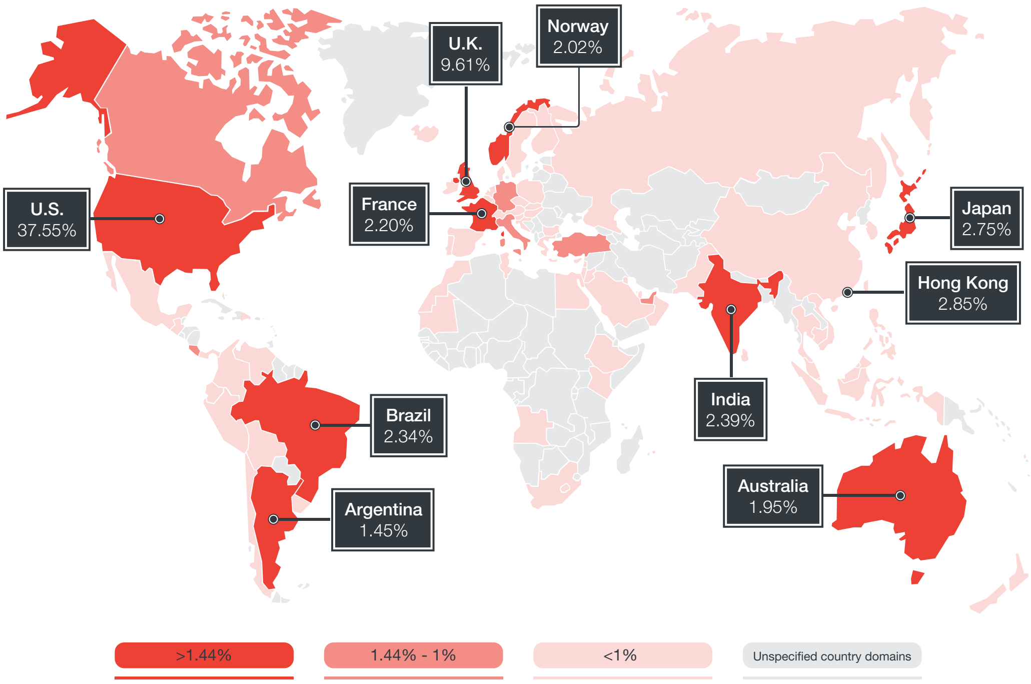


Figure 22: Countries most affected by BEC scams in 2016

Vulnerabilities discovered in widely used devices, including Supervisory Control and Data Acquisition (SCADA) equipment, also surpassed volume records, pushing security researchers and malicious actors to race to find weak points in systems.

2016 also bore witness to the biggest data breach in history, which exposed issues in how companies handled user data. Other organizations, meanwhile, felt the effects of poor IoT security with the onset of massive distributed denial-of-service (DDoS) attacks via botnets like Mirai. The demise of the Angler Exploit Kit gave rise to other kits, which along with ATM malware like Skimer and Alice, continued to pose challenges to businesses' security posture.

PPPs continued to prove worthwhile in the fight against cybercrime, as 2016 bore witness to more cybersecurity wins, including the arrest of one of the most prolific payment card data traffickers, Roman Seleznev (aka Track2, Bulba, nCuX, or psycho), and a BEC scam mastermind (aka Mike). The yearend was also marked by the takedown of another criminal network—Avalanche.

12 APRIL 2016
First Trend Micro-Europol joint research effort, "ATM Malware on the Rise"

05 JULY 2016
Notorious PoS device hacker, Roman Seleznev (aka Track2/Bulba/nCuX/psycho), was arrested

U.S. Secret Service

05 DECEMBER 2016
Avalanche criminal network was taken down

FBI with Trend Micro and other partners

20 APRIL 2016
SpyEye creators, Panin and Bendelladj, were sentenced to a combined 24 years and 6 months in prison

FBI with Trend Micro and other partners

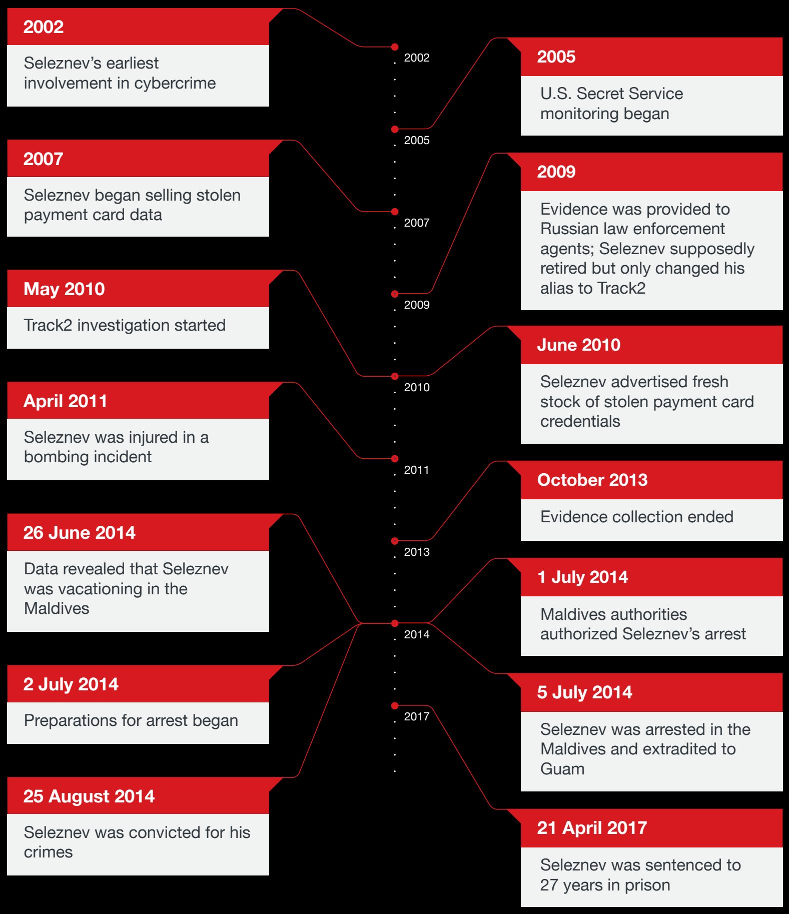
01 AUGUST 2016
BEC scam mastermind, "Mike," was arrested

INTERPOL with Trend Micro and other partners

Figure 23: Cybersecurity wins in 2016

The Crackdown on Track2

The efforts of the U.S. Secret Service led to the arrest and incarceration of Seleznev who was responsible for more than 400 individual network intrusions and marketing and selling hundreds of thousands of stolen payment card account numbers and other financial data in underground markets. Seleznev illicitly earned US$169 million from victims and compromised more than 3,000 banking and financial institutions.



2002
Seleznev's earliest involvement in cybercrime

2005
U.S. Secret Service monitoring began

2007
Seleznev began selling stolen payment card data

2009
Evidence was provided to Russian law enforcement agents; Seleznev supposedly retired but only changed his alias to Track2

May 2010
Track2 investigation started

June 2010
Seleznev advertised fresh stock of stolen payment card credentials

April 2011
Seleznev was injured in a bombing incident

October 2013
Evidence collection ended

26 June 2014
Data revealed that Seleznev was vacationing in the Maldives

1 July 2014
Maldives authorities authorized Seleznev's arrest

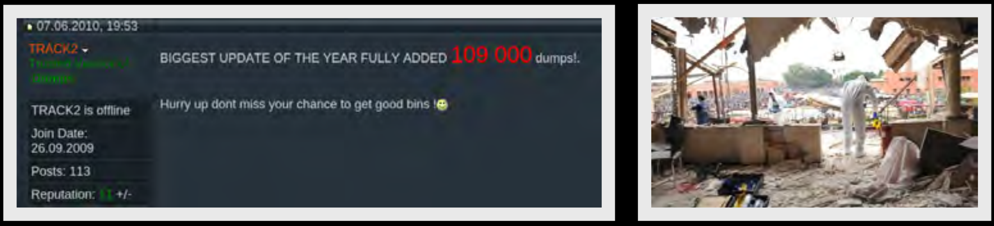
2 July 2014
Preparations for arrest began

5 July 2014
Seleznev was arrested in the Maldives and extradited to Guam

25 August 2014
Seleznev was convicted for his crimes

21 April 2017
Seleznev was sentenced to 27 years in prison

Figure 24: Track2 investigation time line



07.06.2010, 19:53

TRACK2
[illegible]

TRACK2 is offline

Join Date: 26.09.2009

Posts: 113

Reputation: [illegible] +/-

BIGGEST UPDATE OF THE YEAR FULLY ADDED 109 000 dumps!.

Hurry up dont miss your chance to get good bins !

Figure 25: Evidence gathered on Track2

2017:
Ransomware Reigned Supreme

Susceptibility tied the threats of 2017 together. The year showed that systems, platforms, and people were all at risk of security threats. Global ransomware outbreaks that banked on the year's nastiest variants, WannaCry and Petya, cost enterprises huge sums of money and lost information.

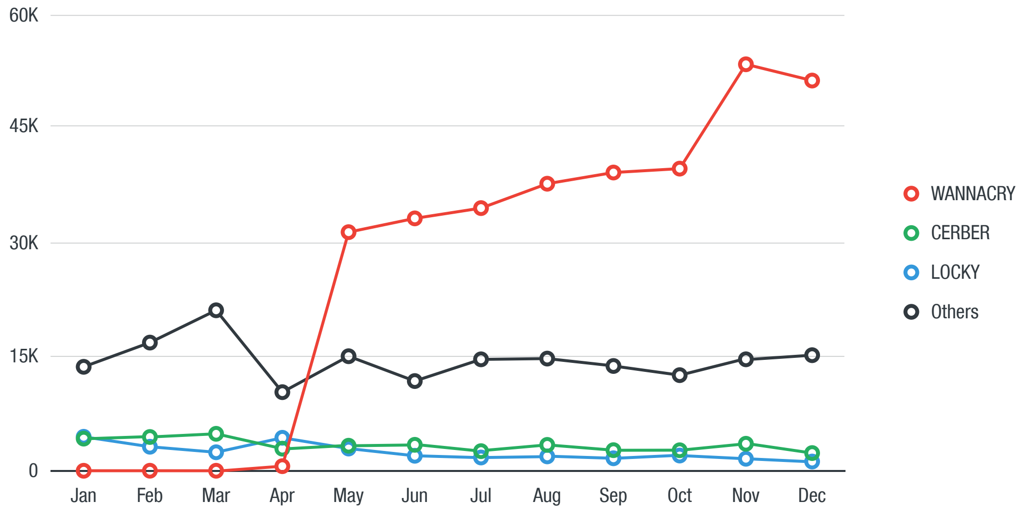
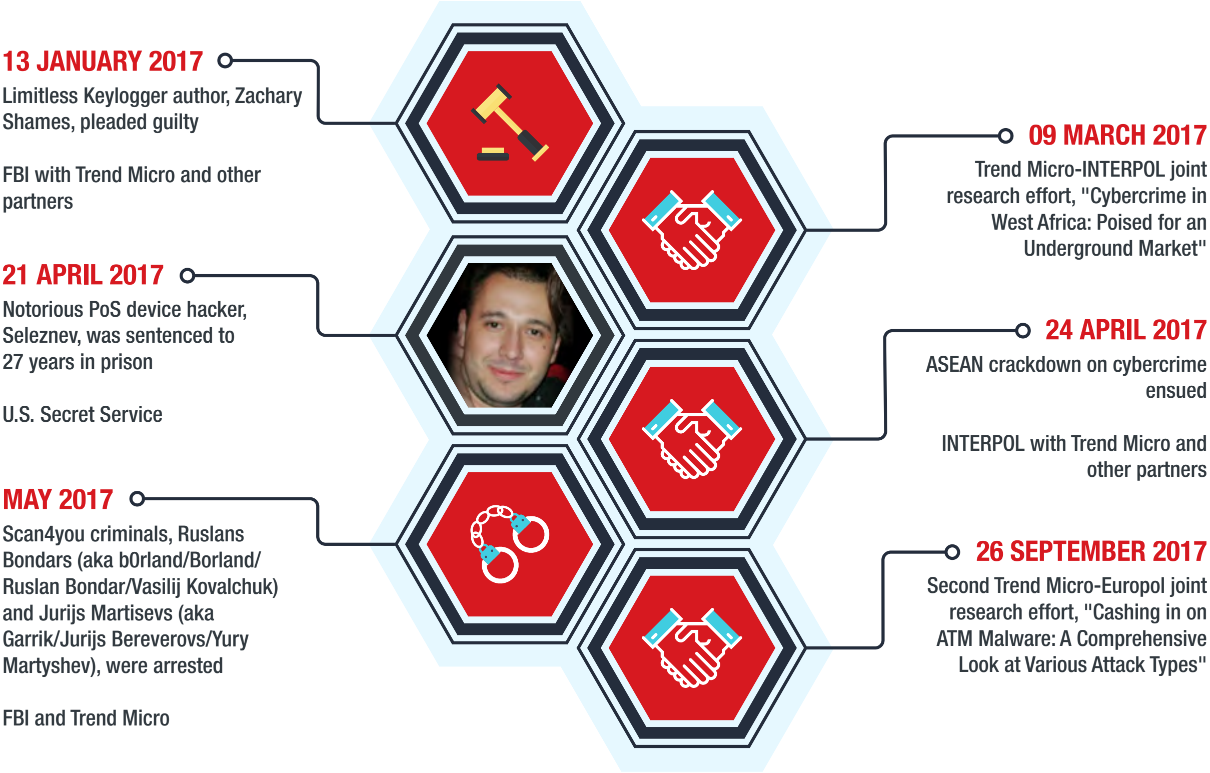


Figure 26: WannaCry volume upsurge in 2017

In April, the Shadow Brokers hacker group leaked reportedly National Security Agency exploits, EternalBlue and EternalRomance, which later on figured in major threat campaigns like the WannaCry, Petya, and Bad Rabbit attacks. On the mobile device front, vulnerabilities like Dirty COW gave users quite a scare as well. The year also witnessed a rise in the volume of zero-day vulnerabilities discovered in SCADA systems.

While BEC scams continued to challenge enterprises, woes brought on by cryptocurrency mining and other threats' meteoric ascent to 2017's list of top threats plagued normal users. Cryptocurrency platforms, mobile devices, and even social media were all affected by miners and similar threats. IoT botnets continued to cause large-scale DDoS attacks akin to Mirai. And despite the drop in data breach disclosures, even more enterprise records ended up in attackers' hands. Equifax and Uber were just two of the well-known companies that lost customer data to hackers.

All was not lost, however, as the crackdown on cybercrime continued with the arrest of Ruslans Bondars (aka b0rland, Borland, Ruslan Bondar, or Vasilij Kovalchuk) and Jurijs Martisevs (aka Garrik, Jurijs Bereverovs, or Yury Martyshev), the conviction of Zachary Shames, Selevnev's sentencing, and the regionwide cleanup effort of sites in Southeast Asia.



13 JANUARY 2017

Limitless Keylogger author, Zachary Shames, pleaded guilty

FBI with Trend Micro and other partners

21 APRIL 2017

Notorious PoS device hacker, Seleznev, was sentenced to 27 years in prison

U.S. Secret Service

MAY 2017

Scan4you criminals, Ruslans Bondars (aka b0rland/Borland/Ruslan Bondar/Vasilij Kovalchuk) and Jurijs Martisevs (aka Garrik/Jurijs Bereverovs/Yury Martyshev), were arrested

FBI and Trend Micro

09 MARCH 2017

Trend Micro-INTERPOL joint research effort, "Cybercrime in West Africa: Poised for an Underground Market"

24 APRIL 2017

ASEAN crackdown on cybercrime ensued

INTERPOL with Trend Micro and other partners

26 SEPTEMBER 2017

Second Trend Micro-Europol joint research effort, "Cashing in on ATM Malware: A Comprehensive Look at Various Attack Types"

Figure 27: Cybersecurity wins in 2017

2018:
The Current Reality

In 2018, digital extortion will be at the core of most cybercriminals' business models, pushing them to get their hands on potentially heftier payouts. Though the global outbreaks of 2017's scale will be few and far between, we do not expect ransomware to disappear this year. Instead, the success of ransomware attacks will serve as catalyst for more damaging campaigns. Cybercriminals may opt to target an organization, possibly in an Industrial IoT environment, to get the biggest bang for their buck. Extortion will also come into play with the General Data Protection Regulation (GDPR) implementation. Attackers may target private data covered by the regulation and ask companies to pay an extortion fee rather than risk punitive fines of up to 4 percent of their annual turnover. This will drive a rise in breach attempts and ransom demands. We also expect the GDPR to be used as a social engineering lure the same way copyright violations (FAKEAV) and police warnings (ransomware) were in campaigns.

IoT vulnerabilities will expand the attack surface as connected devices gain ubiquity. Apart from Mirai-like DDoS attacks, cybercriminals will also use IoT devices as proxies to hide their location and web traffic, especially as most of them are not secure by design. We expect reports of drone-related accidents or collisions as well. Wireless speakers and voice assistants can also help hackers locate target houses for physical break-ins. Cases of biohacking via wearables and medical devices will also materialize. Even life-sustaining pacemakers riddled with vulnerabilities can be exploited for potentially fatal attacks.

BEC scams will ensnare more organizations to fork over their money to attackers. We foresee BEC incidents leading to more than US$9 billion* in global losses. Company executives will continue to be impersonated to wire varying sums of money in attacks. Instead of planting keyloggers, BEC scammers will continue using phishing .PDF files and sites to compromise accounts at lower costs.

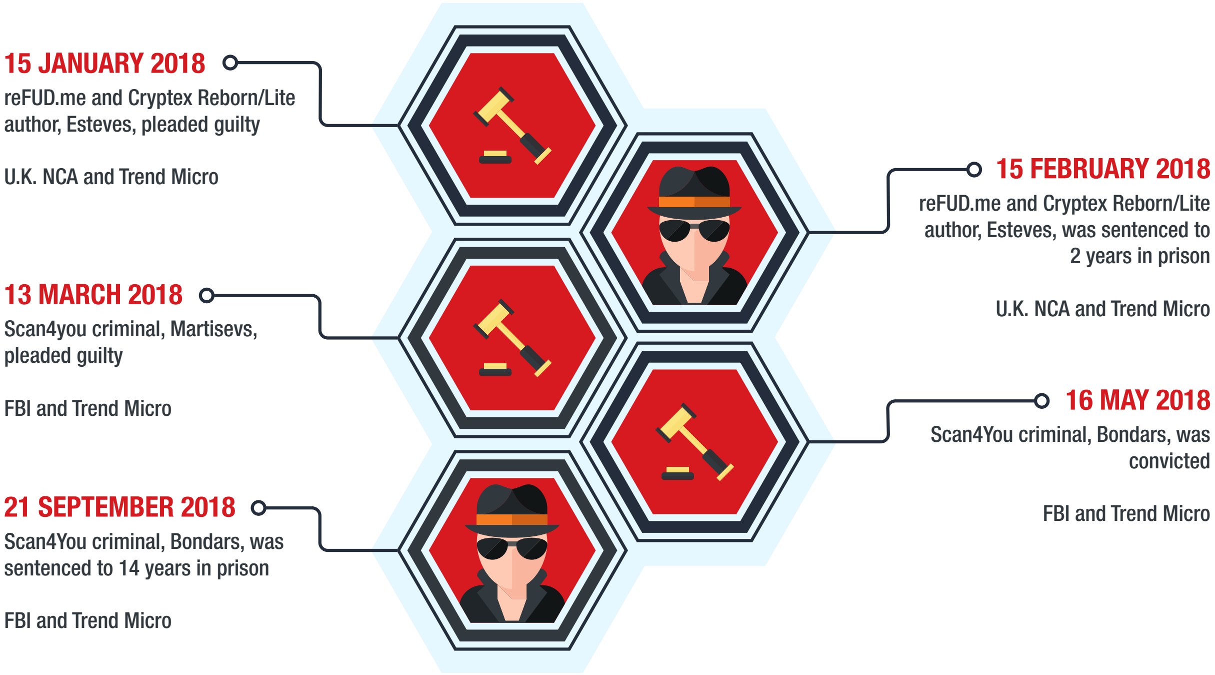
The age of fake news and cyberpropaganda will persist with old-school cybercriminal techniques. We expect cyberpropaganda to spread via tried-and-tested spamming tactics. Manipulated political campaigns will continue to figure in smear tactics and deliberately shift public perception using tools and services that are readily available in underground markets.

* US$9 billion is based on computing the monthly average of reported losses from June to December 2016 and multiplying it by 12. This only assumes that there is a flat growth for reported BEC incidents and victims.

Machine learning and blockchain applications will bring both promises and pitfalls. Moving forward, machine learning will be a key component of security solutions. While it enables more accurate and targeted decision-making, it also runs the risk of being outwitted by malware. The same is true for blockchain technology, which though expected to revolutionize business models, can also be abused for the anonymity that it provides.

Companies will face the challenge of keeping up with the directives of the GDPR prior to enforcement. Laggards will only fully comply if regulators impose fines. Data privacy watchdogs, meanwhile, can interfere with business operations by banning companies from processing certain data. Lawsuits may also come into the picture.

Apart from vulnerability challenges, loopholes in internal processes will also be abused for production sabotage. While real-world processes will allow enterprises to address physical performance issues, their virtual production networks can be maliciously manipulated to disrupt operations or even cause damage. We also expect to find new security flaws in widely used platforms, as attackers renew their focus on browser-based and server-side vulnerabilities to deliver more destructive payloads.



15 JANUARY 2018
reFUD.me and Cryptex Reborn/Lite author, Esteves, pleaded guilty

U.K. NCA and Trend Micro

15 FEBRUARY 2018
reFUD.me and Cryptex Reborn/Lite author, Esteves, was sentenced to 2 years in prison

U.K. NCA and Trend Micro

13 MARCH 2018
Scan4you criminal, Martisevs, pleaded guilty

FBI and Trend Micro

16 MAY 2018
Scan4You criminal, Bondars, was convicted

FBI and Trend Micro

21 SEPTEMBER 2018
Scan4You criminal, Bondars, was sentenced to 14 years in prison

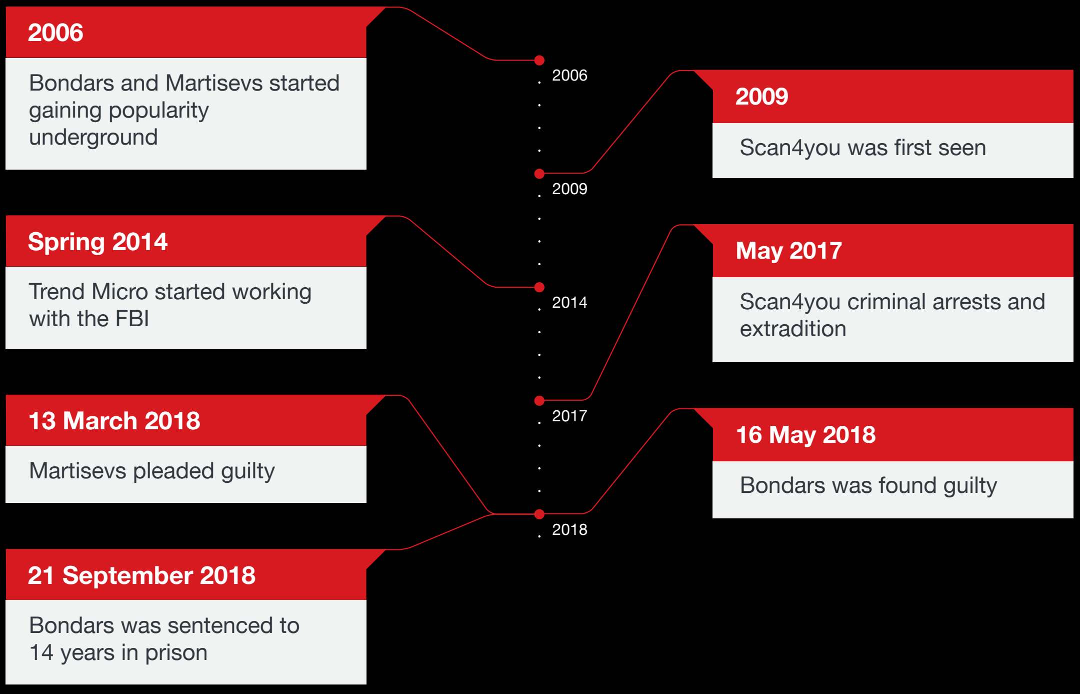
FBI and Trend Micro

Figure 28: Cybersecurity wins in 2018

The Scan4you Takedown

Sometime in May 2017, the FBI arrested and extradited two of the major players in the Scan4you criminal venture, Bondars and Martisevs. Scan4you has been offering counter-antivirus services to criminals since at least 2009. They have been engaging in criminal endeavors since 2006. They have been involved in ventures like Eva Pharmacy, which illegally sold prescription and non-Food and Drug Administration-approved drugs; launched banking malware attacks; and sold stolen payment card credentials in the past.

Martisevs, in his hearing, revealed that one of Scan4you's customers included serious cybercrime perpetrators like those involved in a massive breach attack in November 2013. Bondars, was sentenced to 14 years in prison for his involvement on 21 September 2018.



2006
Bondars and Martisevs started gaining popularity underground

2009
Scan4you was first seen

Spring 2014
Trend Micro started working with the FBI

May 2017
Scan4you criminal arrests and extradition

13 March 2018
Martisevs pleaded guilty

16 May 2018
Bondars was found guilty

21 September 2018
Bondars was sentenced to 14 years in prison

Figure 29: Scan4you case time line

Public-Private Partnerships Versus Cybercrime

If the past 15 years or so is any indication, forging PPPs is the best way to fight against cybercrime. And there are various reasons why that is so. First, the evidence that the police need to solve a cybercrime may not be on hand; it may instead be held by a private company outside its jurisdiction. Next, in cases where the private company resides in the same locale as the criminal, it may also be more familiar with not just the place's culture but also the laws that govern it. Partnerships are essential to making cross-jurisdiction and -culture cooperation work. Finally, in cybercrime investigations, fewer restrictions may apply to private companies than to national law enforcement agencies.

Cybercrime's ubiquity has pushed even organizations like the World Economic Forum to push PPPs to address the issue in 2016. Four elements that would make PPPs work against cybercrime were identified—information sharing, cooperation, adherence to and harmonization of existing laws, and issue discussion and resolution.

To fight cybercrime, the public and private sectors need to create permanent and secure information-sharing channels. Information on hacking cases, new modus operandi, investigation experiences, prosecution details, technical prevention and protection measures, technological development trends and advancements, and IT best practices should flow freely between sectors. Creating a common cybercrime taxonomy and investing in technological innovations to meet future security challenges would also help. Creating global and regional public-private platforms to promote better cooperation between law enforcement authorities and the private sector is also beneficial. The members of both sectors should be encouraged to join and actively engage in existing organizations.

The public and private sectors should also adhere to the mandates of existing cybercrime and related (data privacy, GDPR, etc.) laws. If we are to help secure the digital world, we must strive to harmonize national laws for better cross-border and -cultural collaboration.

To ensure mutual cooperation, trust must be built. Opportunities for discussing and resolving cybercrime issues must be created. Possible obstacles to forging PPPs must be identified and obliterated. Incentives may be offered to encourage full cooperation. Capacity-building programs (investigation and forensics training, etc.) can also help reduce barriers to implementation.

Trend Micro and the U.S. Secret Service are both committed to combatting cybercrime. Trend Micro, for its part, has long been assisting law enforcement agencies in cybercrime investigations. Our international partnership with INTERPOL, memorandum of understanding with the U.K. NCA, longstanding representation on industry advisory boards for Europol, and direct contacts within law enforcement agencies in various countries worldwide help us stay true to our mission—making the world safe for the exchange of digital information. It is the U.S. Secret Service's investigative mission, meanwhile, to safeguard the payment and financial systems of the U.S.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. Optimized for leading environments, including Amazon Web Services, Microsoft®, VMware®, and more, our solutions enable organizations to automate the protection of valuable information from today's threats. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection. With almost 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their connected world. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your
Connected World