Решения Fortinet для противодействия современным угрозам

Андрей Терехов, инженер, aterekhov@fortinet.com

Что требует усиления защиты? Cyber Threat Intelligence

Verizon Data Breach Investigations Report - 2018

Frequency of malware vectors

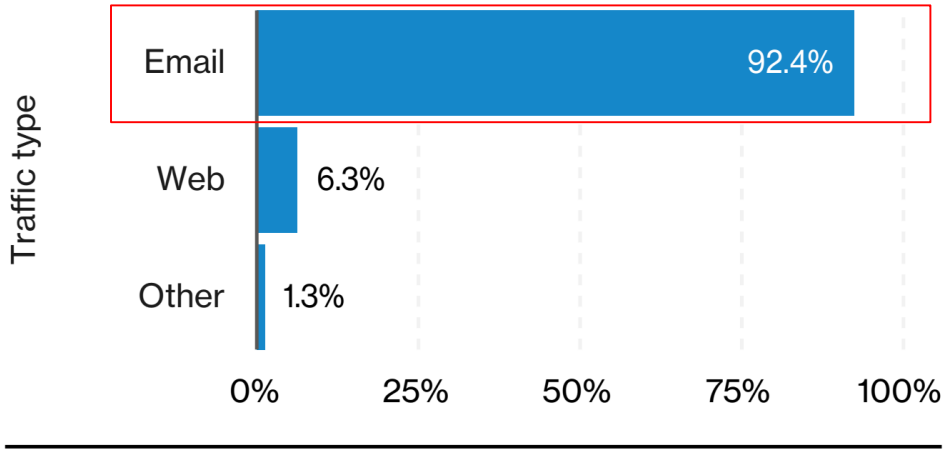


Figure 21. Frequency of malware vectors within detected malware (n=58,987,788)

What are other commonalities?

49% of non-POS malware was installed via malicious email[1]

76% of breaches were financially motivated

13% of breaches were motivated by the gain of strategic advantage (espionage)

68% of breaches took months or longer to discover

https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Что требует усиления защиты? Cyber Threat Intelligence

FBI IC2 - 2017 Internet Crime Report

2017 Crime Types

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Non-Payment/Non-Delivery	84,079	Misrepresentation	5,437
Personal Data Breach	30,904	Corporate Data Breach	3,785
Phishing/Vishing/Smishing/Pharming	25,344	Investment	3,089
Overpayment	23,135	Malware/Scareware/Virus	3,089
No Lead Value	20,241	Lottery/Sweepstakes	3,012
Identity Theft	17,636	IPR/Copyright and Counterfeit	2,644
Advanced Fee	16,368	Ransomware	1,783
Harassment/Threats of Violence	16,194	Crimes Against Children	1,300
Employment	15,784	Denial of Service/TDoS	1,201
BEC/EAC	15,690	Civil Matter	1,057
Confidence Fraud/Romance	15,372	Re-shipping	1,025
Credit Card Fraud	15,220	Charity	436
Extortion	14,938	Health Care Related	406
Other	14,023	Gambling	203
Tech Support	10,949	Terrorism	177
Real Estate/Rental	9,645	Hacktivist	158
Government Impersonation	9,149		

Descriptors*		
Social Media	19,986	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.
Virtual Currency	4,139	

2017 Crime Types *Continued*

By Victim Loss			
Crime Type	Loss	Crime Type	Loss
BEC/EAC	$676,151,185	Misrepresentation	$14,580,907
Confidence Fraud/Romance	$211,382,989	Harassment/Threats of Violence	$12,569,185
Non-Payment/Non-Delivery	$141,110,441	Government Impersonation	$12,467,380
Investment	$96,844,144	Civil Matter	$5,766,550
Personal Data Breach	$77,134,865	IPR/Copyright and Counterfeit	$5,536,912
Identity Theft	$66,815,298	Malware/Scareware/ Virus	$5,003,434
Corporate Data Breach	$60,942,306	Ransomware	$2,344,365
Advanced Fee	$57,861,324	Denial of Service/TDoS	$1,466,195
Credit Card Fraud	$57,207,248	Charity	$1,405,460
Real Estate/Rental	$56,231,333	Health Care Related	$925,849
Overpayment	$53,450,830	Re-Shipping	$809,746
Employment	$38,883,616	Gambling	$598,853
Phishing/Vishing/Smishing/ Pharming	$29,703,421	Crimes Against Children	$46,411
Other	$23,853,704	Hacktivist	$20,147
Lottery/Sweepstakes	$16,835,001	Terrorism	$18,926
Extortion	$15,302,792	No Lead Value	$0
Tech Support	$14,810,080		

		Descriptors*
Social Media	$56,478,483	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.
Virtual Currency	$58,391,810	

https://pdf.ic3.gov/2017_ic3report.pdf

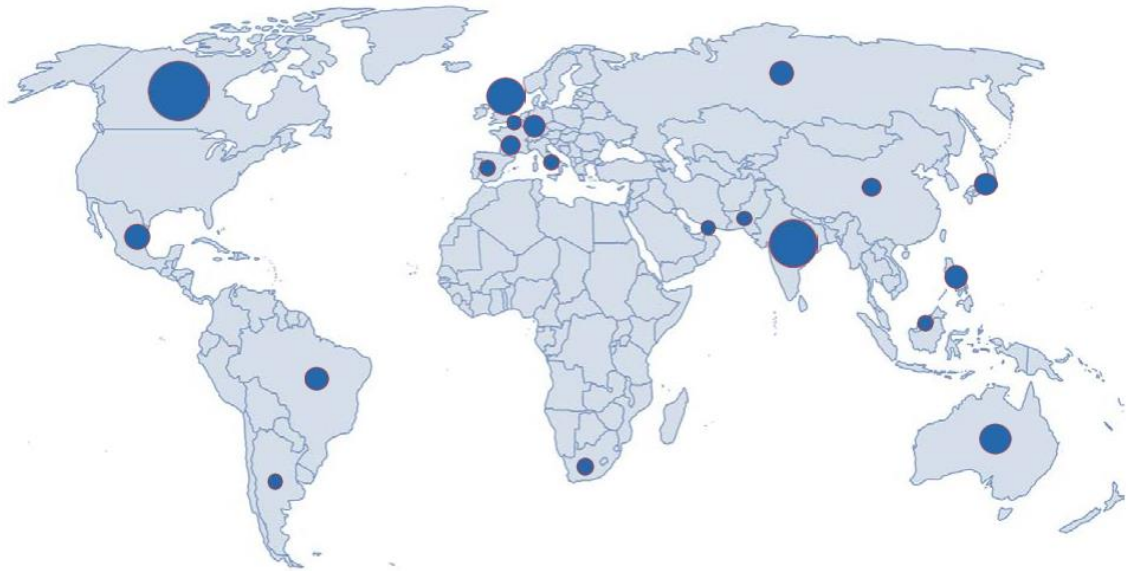
In 2017, IC3 received a total of 301,580 complaints with reported losses exceeding $1.4 Billion

Что требует усиления защиты? Cyber Threat Intelligence

FBI IC2 - 2017 Internet Crime Report

Top 20 Foreign Countries by Victim

Excluding the United States[17]



1. Canada	3,164	6. Russian Federation	594	11. France	368	16. Netherlands	266
2. India	2,819	7. Brazil	558	12. China	366	17. Malaysia	265
3. United Kingdom	1,383	8. Germany	466	13. South Africa	349	18. United Arab Emirates	259
4. Australia	989	9. Philippines	453	14. Italy	291	19. Spain	248
5. Mexico	632	10. Japan	413	15. Pakistan	276	20. Argentina	238

Virtual Currency	4,139	tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.

2017 Crime Types *Continued*

By Victim Loss			
Crime Type	**Loss**	**Crime Type**	**Loss**
BEC/EAC	$676,151,185	Misrepresentation	$14,580,907
Confidence Fraud/Romance	$211,382,989	Harassment/Threats of Violence	$12,569,185
Non-Payment/Non-Delivery	$141,110,441	Government Impersonation	$12,467,380
Investment	$96,844,144	Civil Matter	$5,766,550
Personal Data Breach	$77,134,865	IPR/Copyright and Counterfeit	$5,536,912
Identity Theft	$66,815,298	Malware/Scareware/ Virus	$5,003,434
Corporate Data Breach	$60,942,306	Ransomware	$2,344,365
Advanced Fee	$57,861,324	Denial of Service/TDoS	$1,466,195
Credit Card Fraud	$57,207,248	Charity	$1,405,460
Real Estate/Rental	$56,231,333	Health Care Related	$925,849
Overpayment	$53,450,830	Re-Shipping	$809,746
Employment	$38,883,616	Gambling	$598,853
Phishing/Vishing/Smishing/ Pharming	$29,703,421	Crimes Against Children	$46,411
Other	$23,853,704	Hacktivist	$20,147
Lottery/Sweepstakes	$16,835,001	Terrorism	$18,926
Extortion	$15,302,792	No Lead Value	$0
Tech Support	$14,810,080		

		Descriptors*
Social Media	$56,478,483	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.
Virtual Currency	$58,391,810	

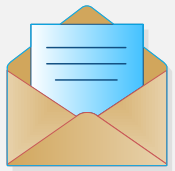
https://pdf.ic3.gov/2017_ic3report.pdf

In 2017, IC3 received a total of 301,580 complaints with reported losses exceeding $1.4 Billion

Усиления защиты требует электронная почта
«Но у нас же уже есть антиспам?»

Усиления защиты требует электронная почта
«Но у нас же уже есть антиспам?»

Методы и тактики злоумышленников



Плохое

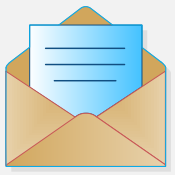
Последовательный поиск новых и «**новых**» атак – обход репутации и сигнатур

Использование эксплоитов для запуска кода без взаимодействия с пользователем

Социальная инженерия – обман даже опытных пользователей

Усиления защиты требует электронная почта
«Но у нас же уже есть антиспам?»

Виды атак на электронную почту, обходящих репутацию и сигнатуры



Плохое

Business Email Compromise:
цель – мошенничество,
побудить к переводу денег

Zero day vulnerabilities:
Цель – заражение вредоносным ПО за счёт эксплуатации 0-day

Phishing и Spear Phishing:
цель – побудить пользователя к действию: открытие файла, переход по ссылке, загрузка «обновления», ввод логина-пароля

David Finger, fortinet.com blog, April 26, 2018

Усиления защиты требует электронная почта «Но у нас же уже есть антиспам?»

Насколько они эффективны?

Плохое

Статистика за один месяц 2018:

	Частота	В день в организации с 1000 человек, получающих каждый по 50 писем в день
Фишинг	1/3331	15
Новое ВПО	1/645	77

Osterman Research White Paper, 04'2018

27% в среднем пользователей попадаются на целенаправленный фишинг

KnowBe4, 2018

4% пользователей в среднем кликнут на любую ссылку

Verizon DBIR, 2018

Усиления защиты требует электронная почта
«Но у нас же уже есть антиспам?»

Наспех собранной армии, вооруженной вилами и копьями, не поможет информация о приближении баллистической ракеты, даже если известна её точная модель и кто её запустил.

https://blogs.gartner.com/anton-chuvakin/2015/08/13/threat-intelligence-and-operational-agility/

Продвинутые угрозы обходят антиспам? Что же делать?

Gartner - Market Guide for Secure Email Gateways

Продвинутые угрозы легко обходят сигнатурные методы, традиционно используемые в шлюзах электронной почты

Gartner

Архитектура современного шлюза электронной почты, позволяющая противостоять продвинутым угрозам

Продвинутые угрозы обходят антиспам? Что же делать?

Gartner - Market Guide for Secure Email Gateways

Продвинутые угрозы легко обходят сигнатурные методы, традиционно используемые в шлюзах электронной почты

Продвинутые угрозы

- С вложениями
- Со ссылками
- Подложный отправитель

Шлюз защиты электронной почты

Защита от продвинутых угроз

- Сетевая песочница/разоружение и реконструкция контента
- Переписывание URL и проверка в момент клика
- Инспекция контента, детектирование спуфинга и аномалий

MTA/анти-спам/сигнатурный антивирус

Катастрофоустойчивость

Архивация

Шифрование

DLP

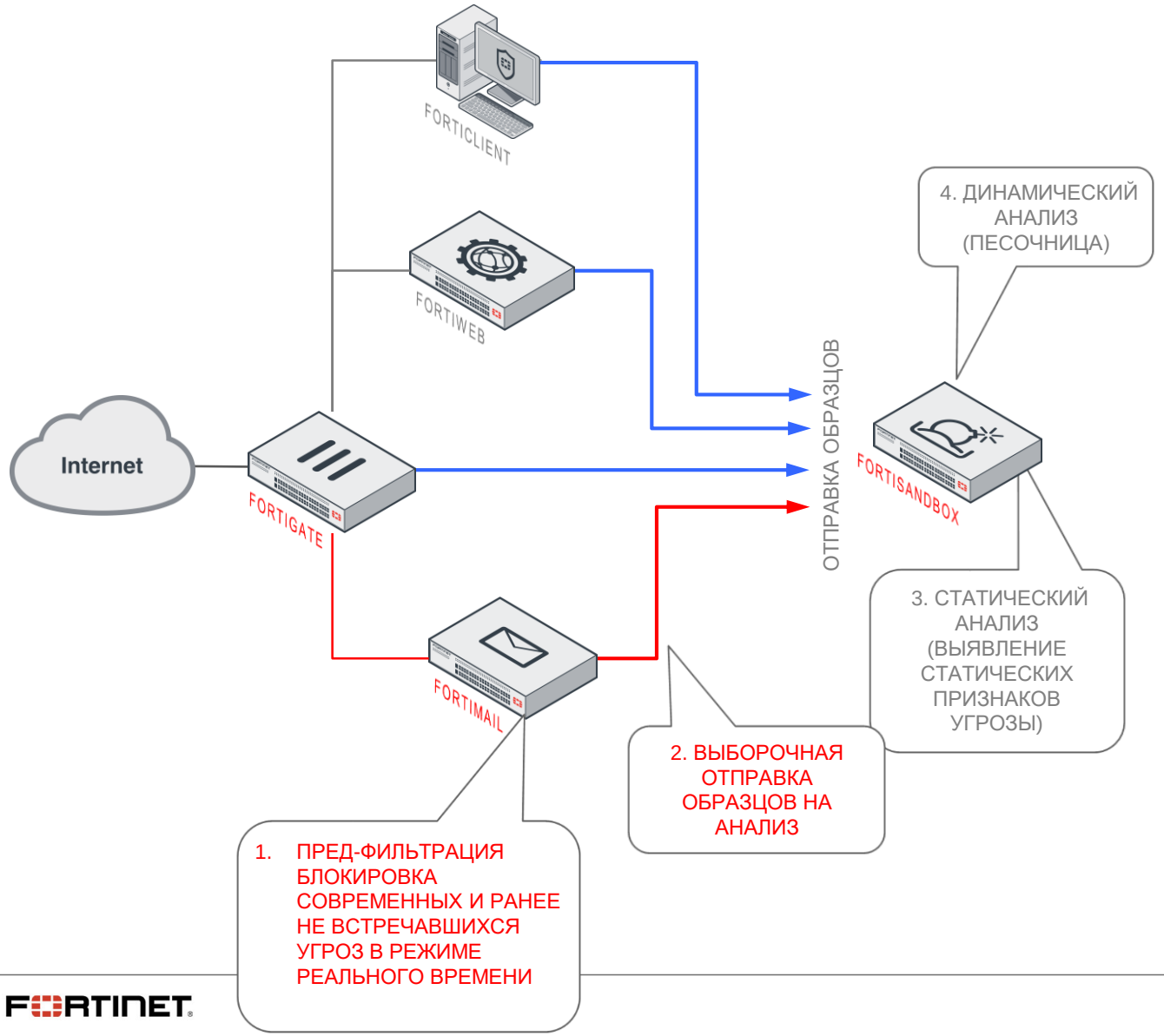

Хорошее


Исходящее

Gartner

Архитектура современного шлюза электронной почты, позволяющая противостоять продвинутым угрозам

Решение от Fortinet - Advanced Threat Protection
Защита от продвинутых угроз



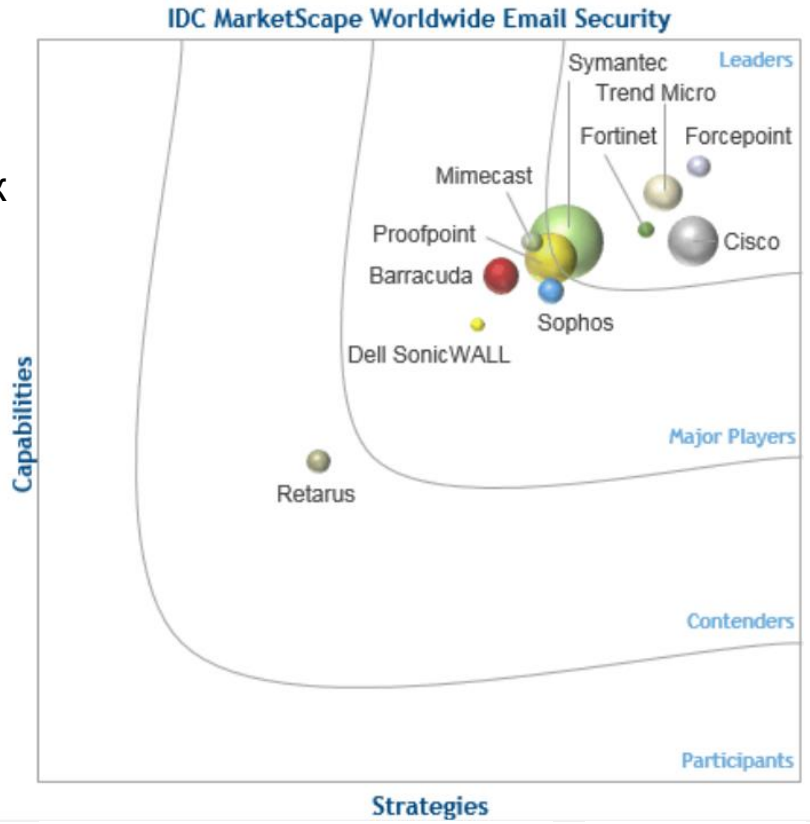
Комплексное решение для защиты от продвинутых угроз:

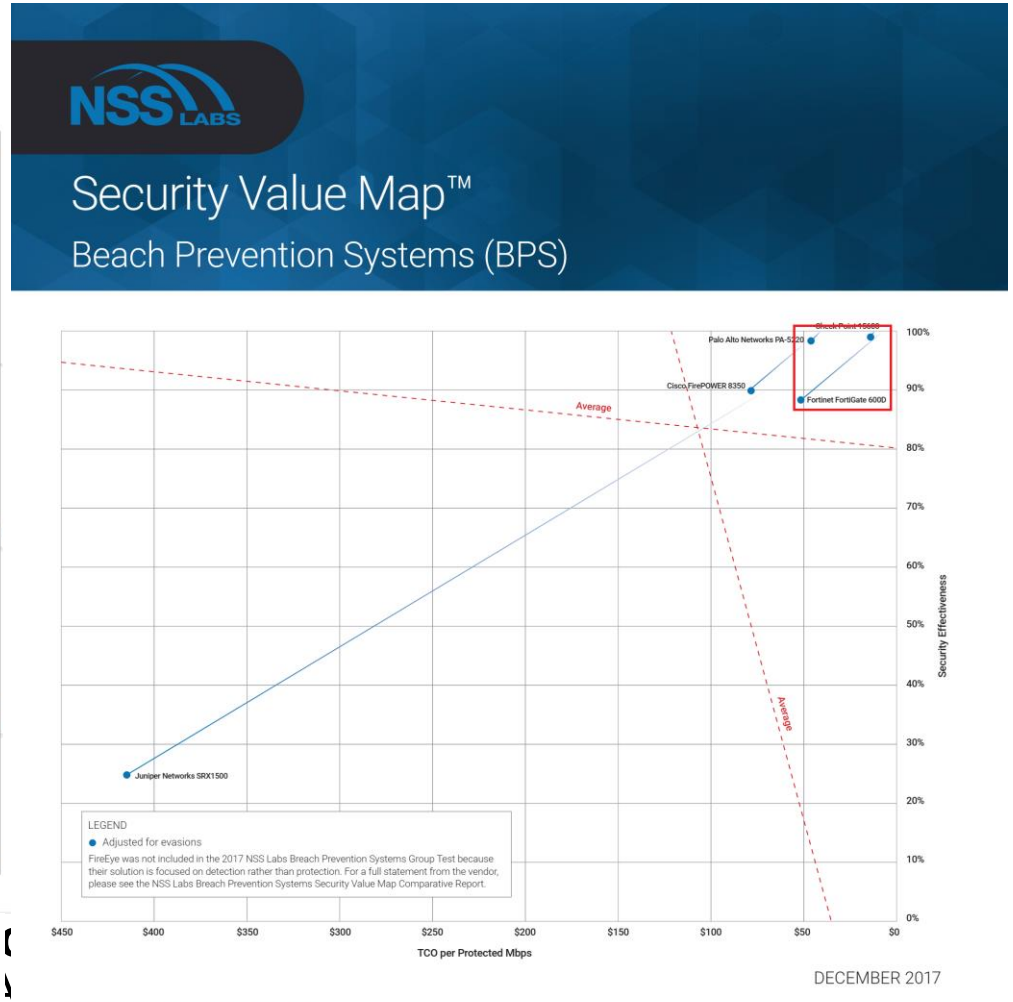
- **FortiSandbox** – сетевая песочница (Network Sandbox), ключевой элемент фабрики безопасности
- **FortiMail** – шлюз защиты электронной почты (Secure Email Gateway)
- **FortiGate** – универсальный шлюз безопасности (Enterprise Firewall)
- **FortiWeb** – межсетевой экран веб-приложений (Web Application Firewall)
- **FortiClient** – средство защиты рабочих станций (Endpoint Protection)
- **FortiADC** – балансировщик нагрузки (ADC)
- **FortiProxy** – веб-шлюз (Secure Web Gateway)

Решение от Fortinet - Advanced Threat Protection
Защита от продвинутых угроз

- Репутационный антивирус и контроль изменения репутации
- Проверка файлов и ссылок в песочнице – предотвращение нового ВПО
- Разоружение и реконструкция контента
- Расшифровка запароленных вложений и архивов
- Проверка ссылок в момент клика (Time-of-Click) – по репутации и в песочнице
- Защита от подложных отправителей (Impostor Protection)

- *И это далеко не всё*





PRODUCTS TESTED

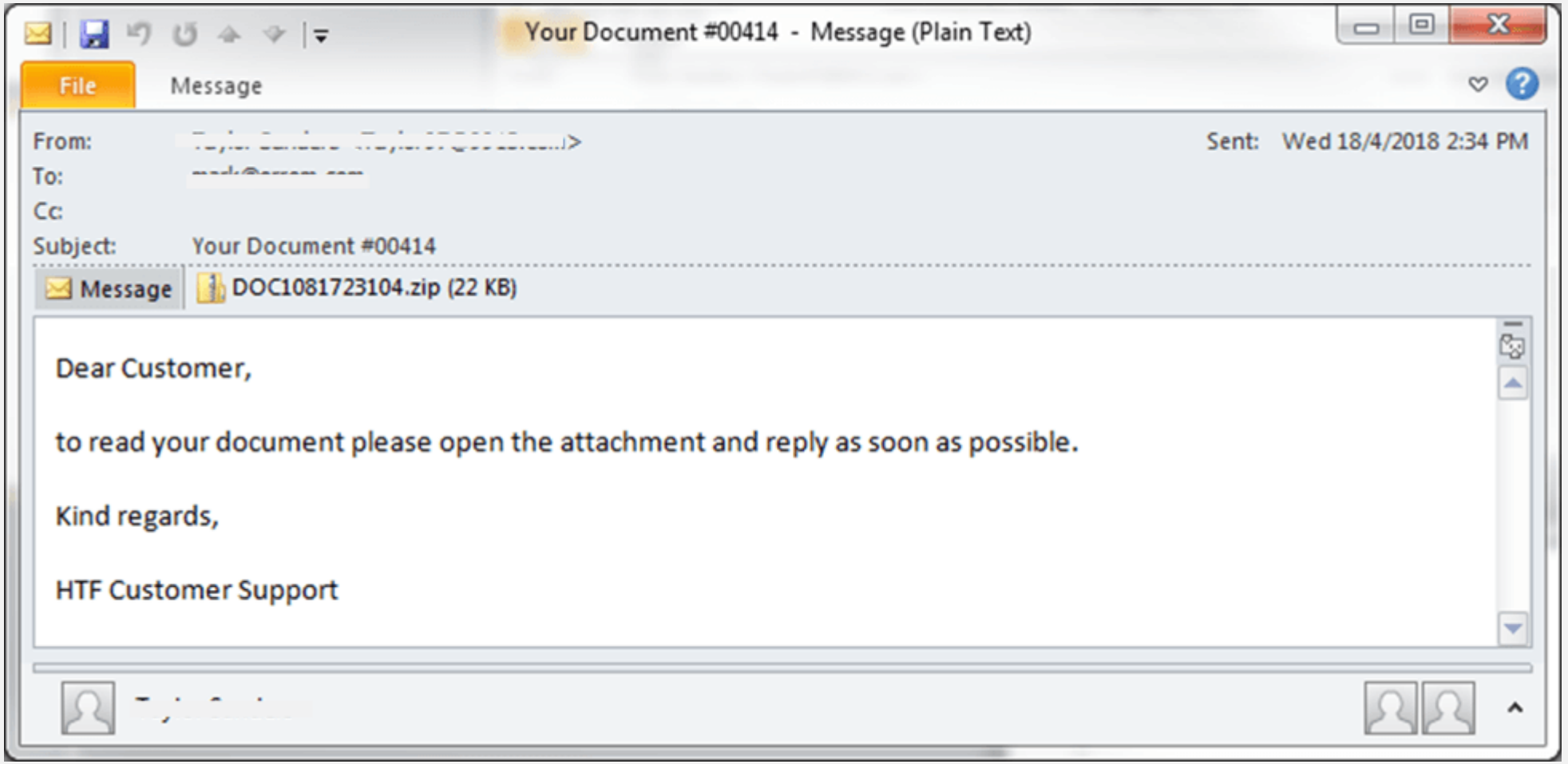
- Check Point Software Technologies 15600 Next Generation Threat Prevention & SandBlast™ (NGTX) Appliance R77.30
- Cisco FirePOWER 8350 v6.1.0.1 with Cisco AMP v5.1.12.10483
- Fortinet Advanced Threat Protection (FortiSandbox Cloud with FortiGate 600D v5.6.1, FortiMail Virtual Appliance v5.4.0 and FortiClient ATP Agent v5.6.1.1112)
- Juniper Networks SRX1500 v15.1X49-D90.7 with Sky ATP
- Palo Alto Networks PA-5220 PAN-OS 8.0.3-h4 with Traps v4.1.0.28239

ATD-Email

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE – EMAIL

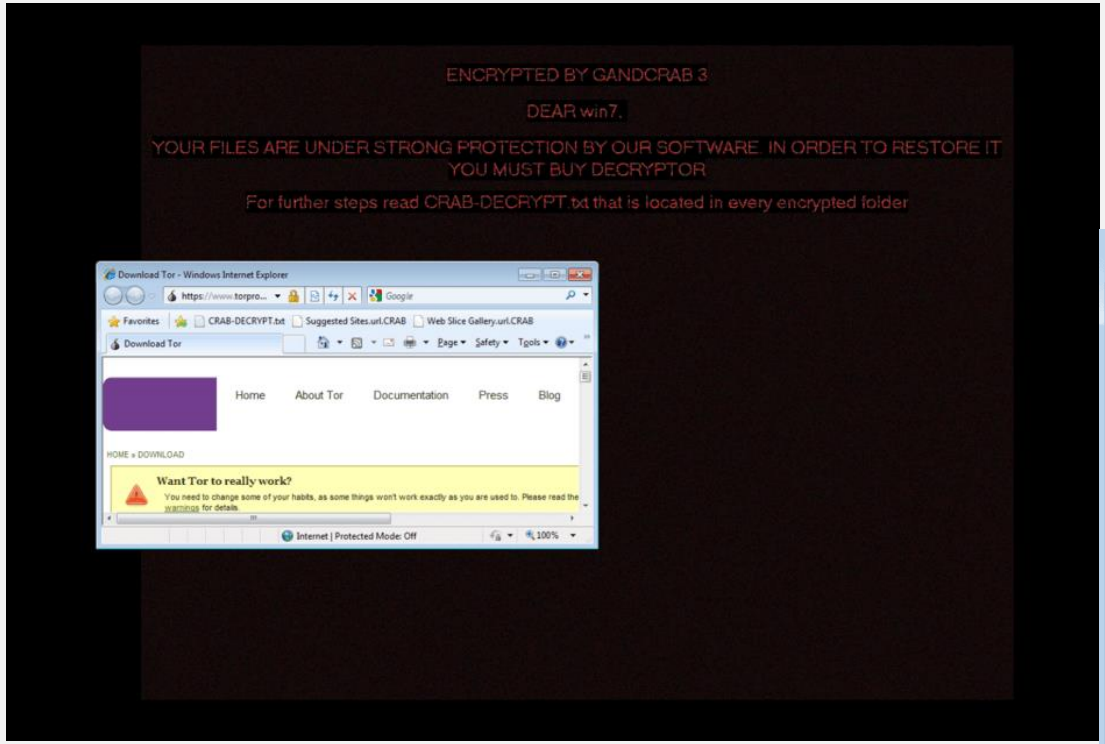
vb VERIFIED SPAM + virusbtn.com

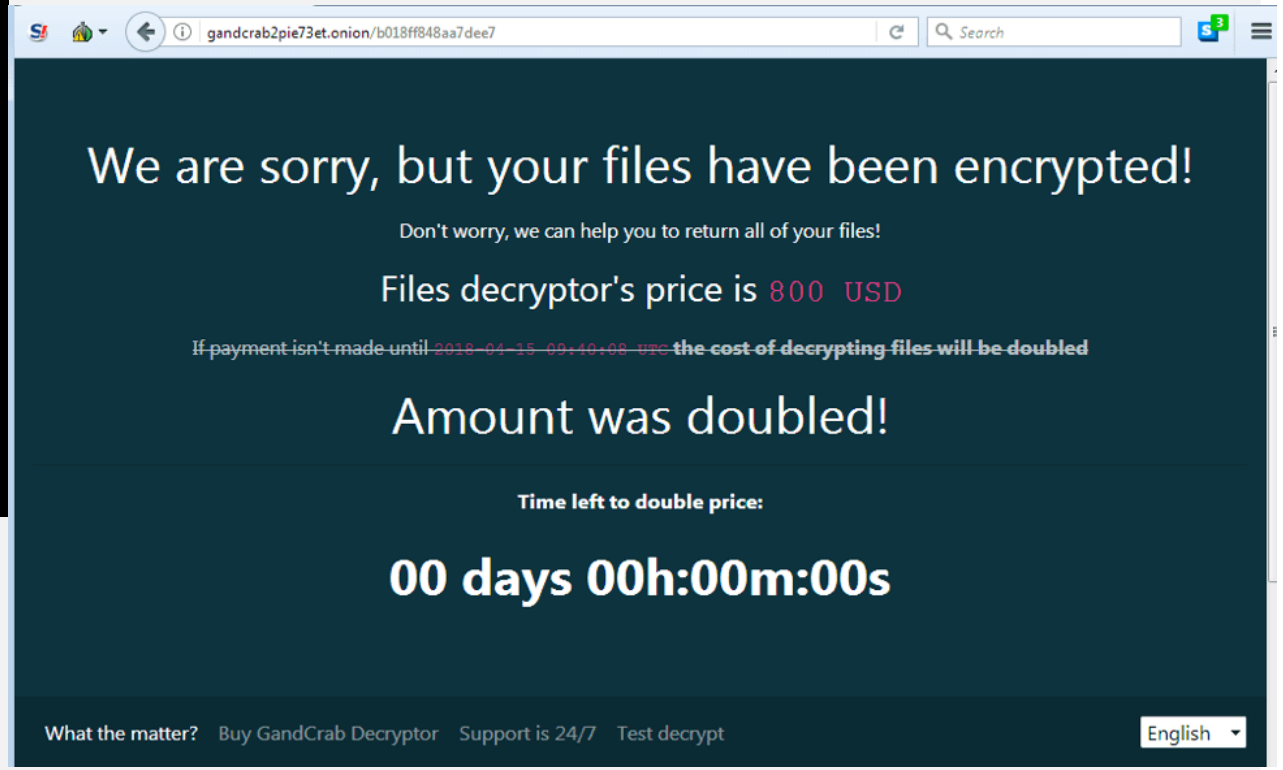
Как защититься от вредоносных вложений? GandCrab



- Наиболее распространенный на сегодняшний день вирус-шифровальщик
- Основной способ доставки – вложение с js-/vbs- загрузчиком в электронной почте

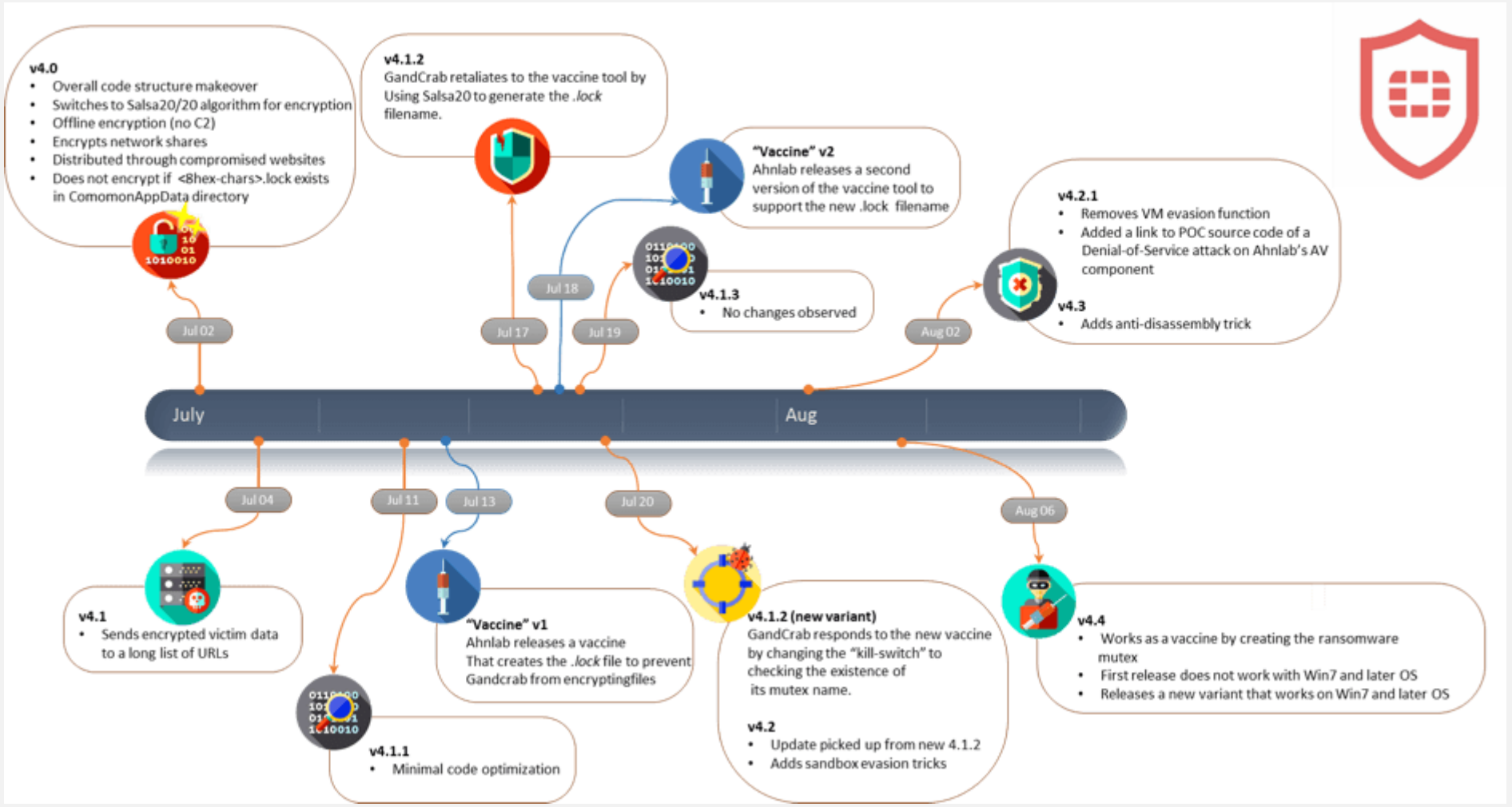
Как защититься от вредоносных вложений? GandCrab





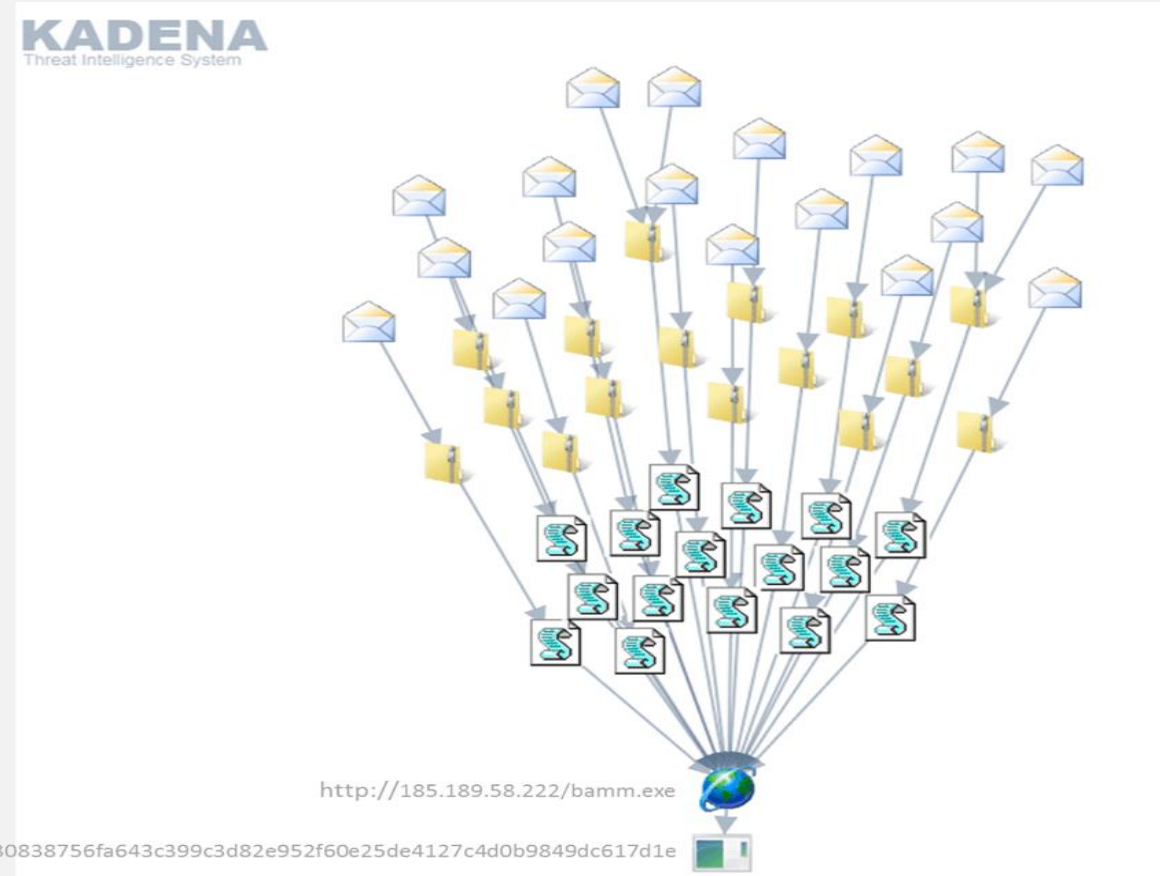
- После открытия – инструкции, страница в Tor

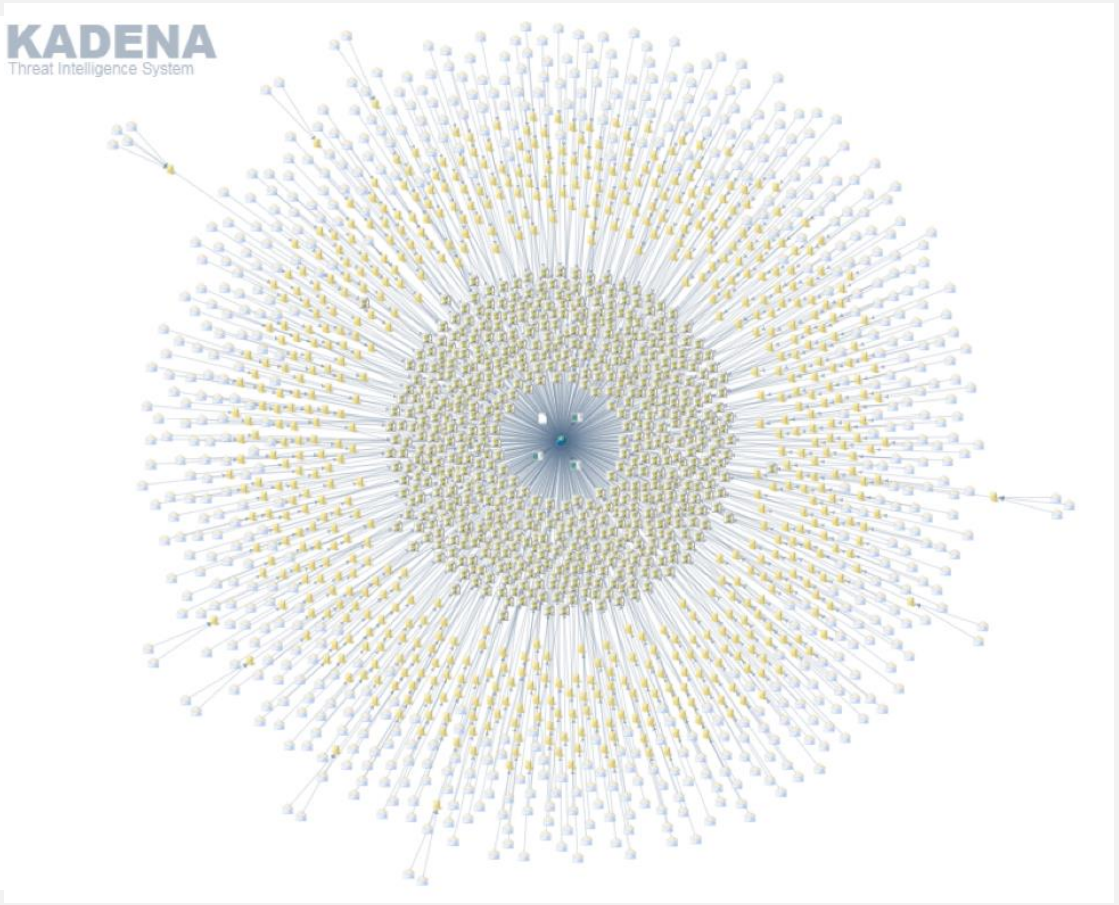
Как защититься от вредоносных вложений? GandCrab



- Появилось в начале 2018 года, активно развивается - 4 версии
- Ransomware-as-a-Service (RaaS)

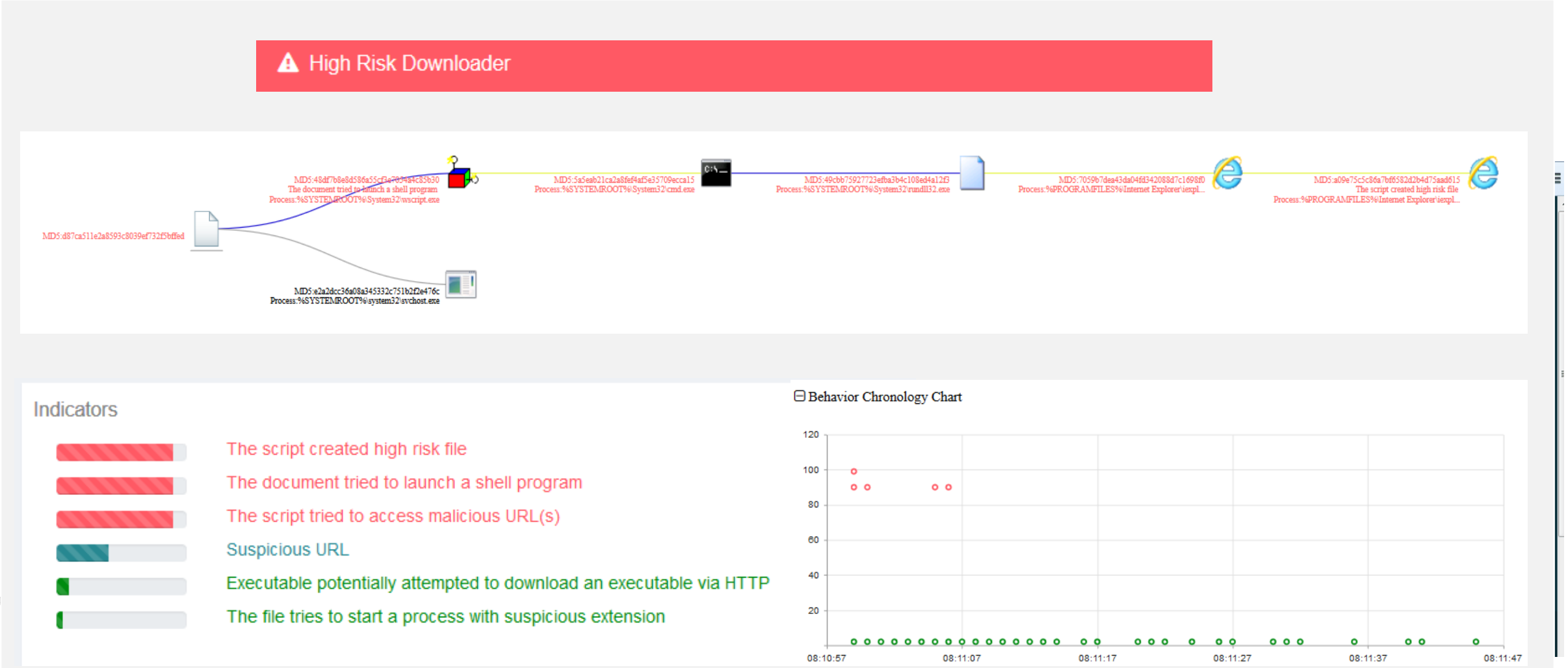
Как защититься от вредоносных вложений? GandCrab





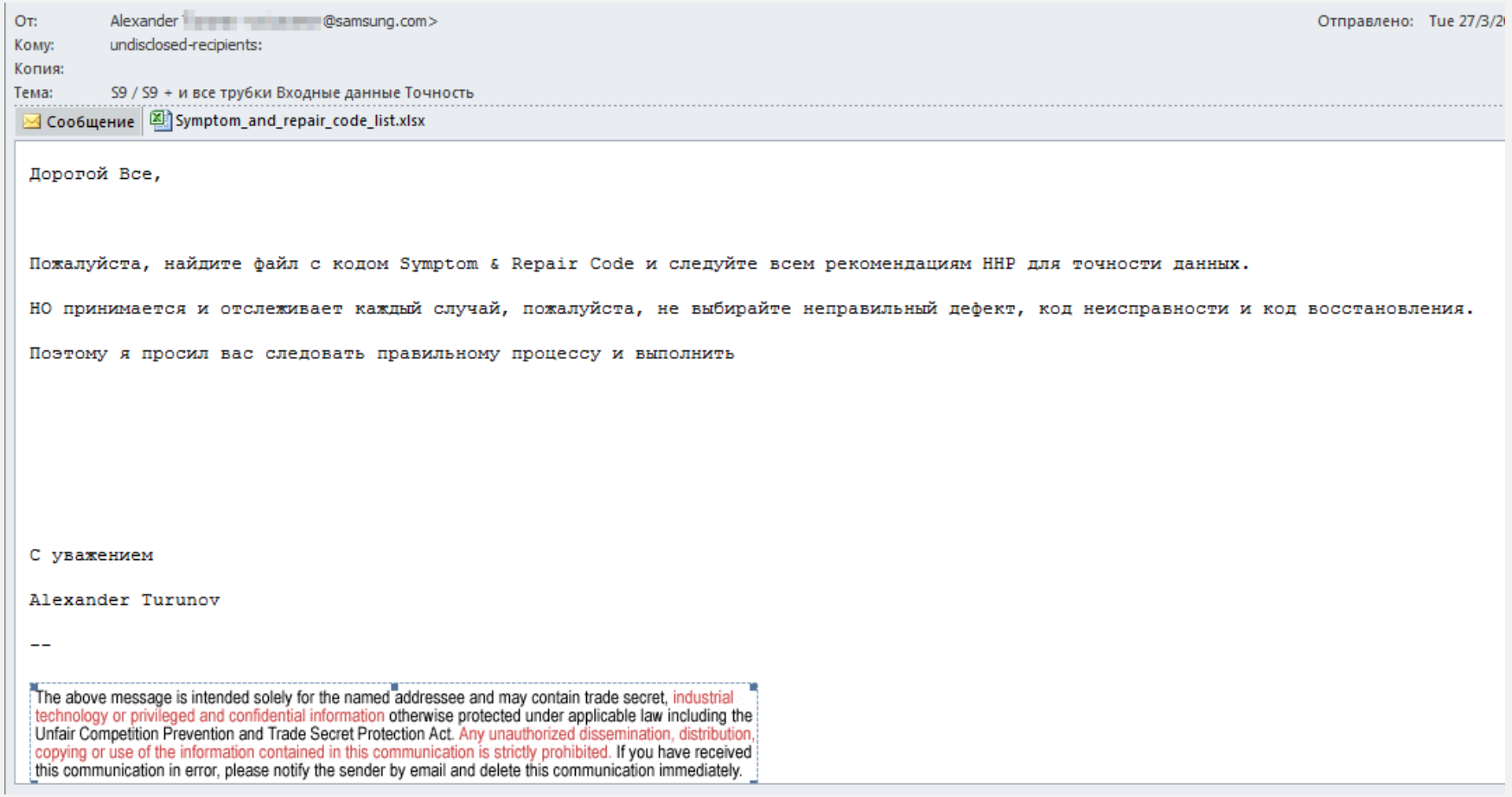
- Почему сигнатурный антивирус на шлюзе бесполезен против такой атаки
- Уникальные загрузчики, часто меняющиеся вредоносные компоненты

Как защититься от вредоносных вложений? GandCrab



- Поэтому необходимо проводить анализ подозрительных вложений в песочнице
- => Выявление ВПО по поведению, предотвращение доставки писем с ВПО

Что делать, если результат нужен быстро?
Атака на сервисные центры мобильных телефонов



От: Alexander [redacted]@samsung.com> Отправлено: Tue 27/3/2
Кому: undisclosed-recipients:
Копия:
Тема: S9 / S9 + и все трубки Входные данные Точность
Сообщение | Symptom_and_repair_code_list.xlsx

Дорогой Все,

Пожалуйста, найдите файл с кодом Symptom & Repair Code и следуйте всем рекомендациям HHP для точности данных.

HO принимается и отслеживает каждый случай, пожалуйста, не выбирайте неправильный дефект, код неисправности и код восстановления.

Поэтому я просил вас следовать правильному процессу и выполнить

С уважением

Alexander Turunov

--

- Рассылка писем с вложениями, якобы содержащими новые служебные коды
- По факту во вложениях эксплоит CVE-2017-11882

Что делать, если результат нужен быстро?
Атака на сервисные центры мобильных телефонов

Header Name	Header Value
X-Yandex-FolderName	Inbox
Return-Path	a.[redacted]@samsung.com
X-Yandex-Front	mxfront2g.mail.yandex.net
X-Yandex-TimeMark	1522128802
Authentication-Results	mxfront2g.mail.yandex.net; spf=softfail (mxfront2g.mail.yandex.net: transitioning domain of samsung.com does not designate 66.[redacted] as permitted sender, rule=[~all]) smtp.mail=a.turunov@samsung.com
X-Yandex-Spam	1
X-Authority-Analysis	v=2.2 cv=cY2iljLM c=1 sm=1 tr=0 a=ip9sk82UPAQ/lpE5utroiw==:117 a=ip9sk82UPAQ/lpE5utroiw==:17 a=v2DPQv5-lfwA:10 a=a9SbwjEakwbGy57HaE8A:9 a=QEXdDO2ut3YA:10 a=hD80L64hAAAA:8 a=ZtfFnOK7jTymUBPpLdcA:9 a=_oPMXimmy9A4AXaI:21 a=_W_S_7VecoQA:10 a=22bfjmUUjbgOyheBHNQA:9 a=w_9GLTjXVB2a76Av:18 a=1Vq_FK4TplAA:10 a=NhVScO-HjH8A:10 a=4qBtGoCUj2RsnWkpVaEA:9 a=IKIoO-ieCDEA:10 a=7qx8gLC0iM8A:10 a=oQrlS-b8-hQA:10 a=ckaI8g68nOMA:10 a=6tzKkkzE5qlo4XtTRTpo:22 a=b4yw5UJVTUN-GkEvK7bM:22 a=X1c0k9nRQnjIoBfxGzdG:22
MIME-Version	1.0
Date	Mon, 26 Mar 2018 23:30:55 -0600
From	Alexander Turunov <a.turunov@samsung.com>
To	undisclosed-recipients:;
Subject	=?UTF-8?Q?S9_/_S9_+_=D0=B8_=D0=B2=D1=81=D0=B5_=D1=82=D1=80=D1=83?= =?UTF-8?Q?=D0=B1=D0=BA=D0=B8_=D0=92=D1=85=D0=BE=D0=B4=D0=BD=D1=8B=D0=B5_?= =?UTF-8?Q?=D0=B4=D0=B0=D0=BD=D0=BD=D1=8B=D0=B5_=D0=A2=D0=BE=D1=87=D0=BD?= =?UTF-8?Q?=D0=BE=D1=81=D1=82=D1=8C?=

- Письма отправлялись якобы от Samsung (header from)
- SPF softfail

Что делать, если результат нужен быстро?
Атака на сервисные центры мобильных телефонов

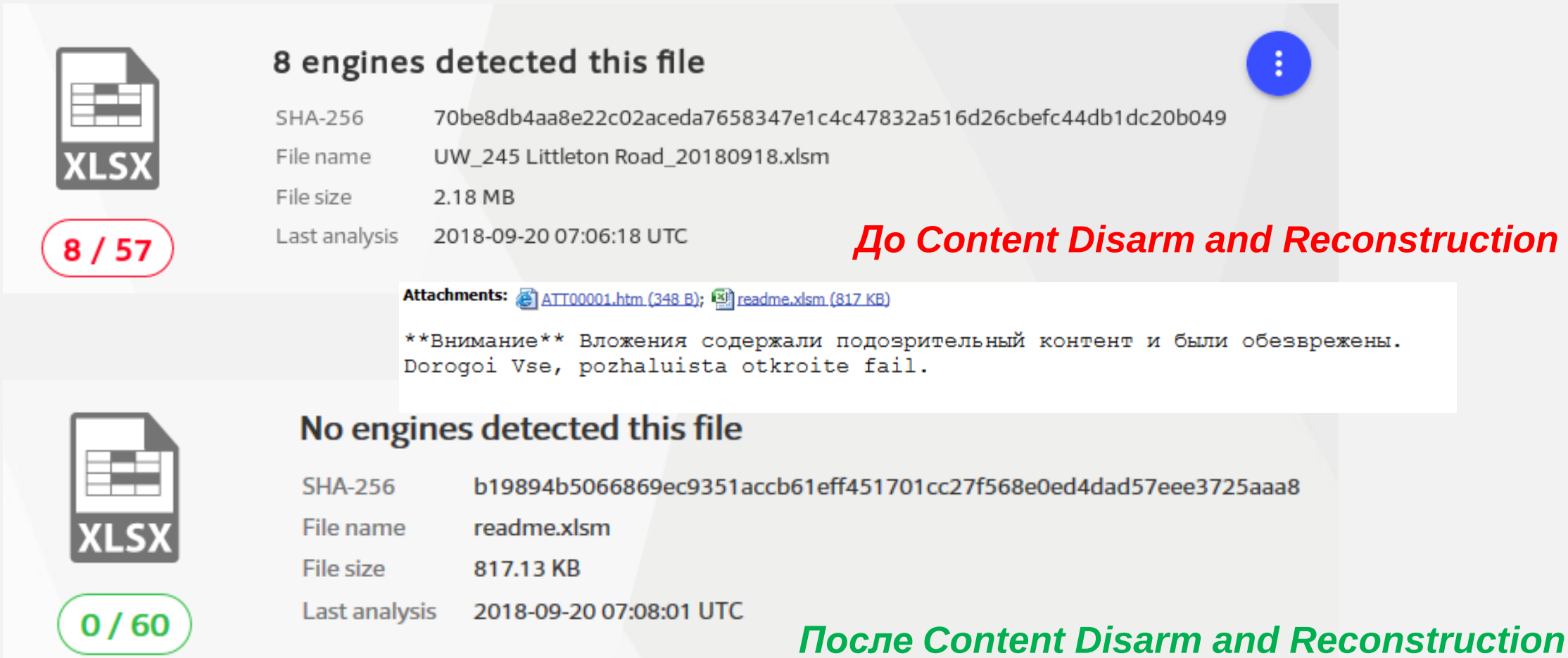
	A	B	C	D	E	F	G
1	Name of the User*	GSPN ID*	Email*	Job Desc	ASC name*	ASC code*	Mobile No.
2	mohamed.moawad	Moawad	Mohamed Moawad Abd ElHalim, MTI Samsung <[redacted]@mti-mmgroup.com>	Technician	[redacted]	[redacted]	[redacted]
3	OMAR EID TAHA	OMAR[redacted]	Omar Eid Taha Morsi, MTI Samsung <[redacted]@mti-mm	Technician	[redacted]	[redacted]	[redacted]
4	Mohamed Adel Bayoumi	ADEL20[redacted]	Mohamed Adel Bayoumi, MTI Samsung <[redacted]	Technician	[redacted]		[redacted]
5							
6							
7							

Protocol	Host	URL	Body	Caching	Content-Type	Process
HTTP	brrange.com	/imm.exe	512	no-cac...	text/html; charset=UTF-8	eqnedt32:3836
HTTP	brrange.com	/imm.exe	512	no-cac...	text/html; charset=UTF-8	eqnedt32:5040
HTTP	brrange.com	/imm.exe	512	no-cac...	text/html; charset=UTF-8	eqnedt32:5080

```
3  // Types:
4  //
5  // Please-contact-abuse@imminentmethods.net-with-the-hardware-id:-"f852b5a7031dec71403fdb426a867bb6"-and-company-
     name:-"test"-if-this-assembly-was-found-being-used-maliciously-.-This-file-was-built-using-Invisible-Mode
6
```

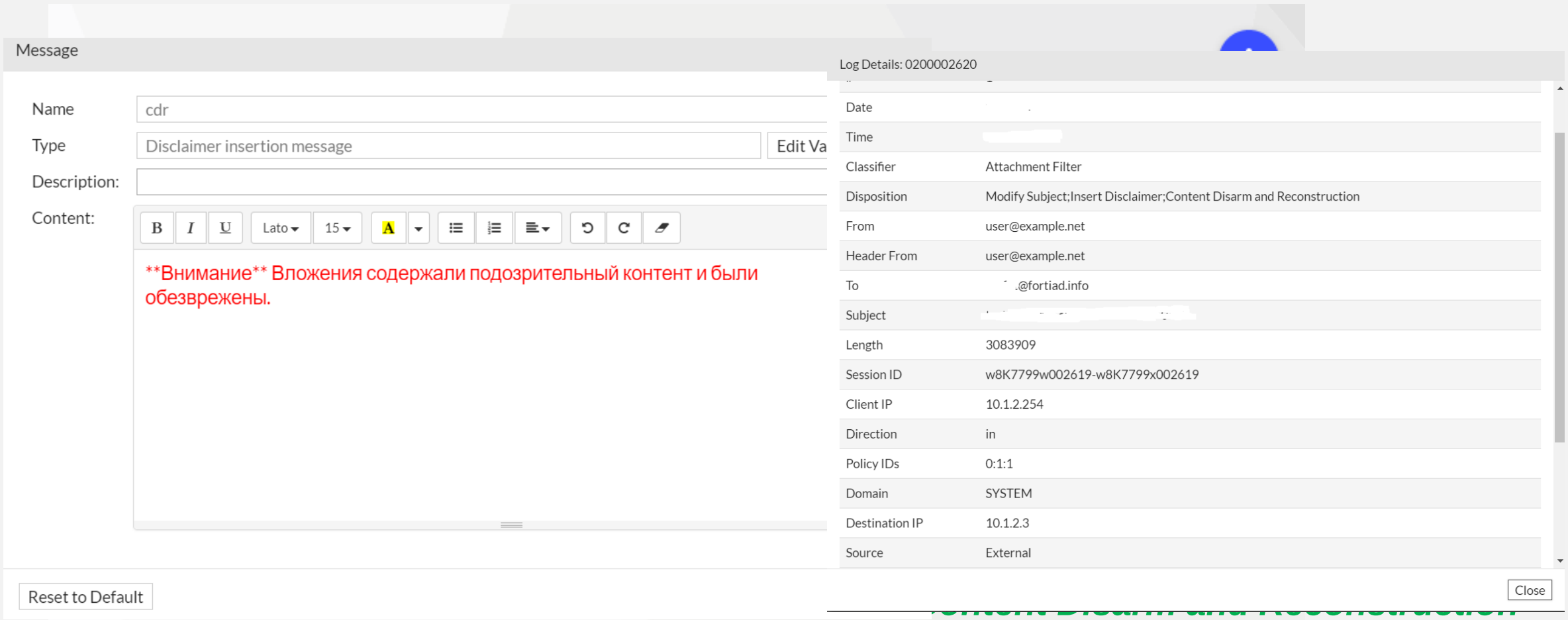
- Содержимое Excel файла похоже на легитимное
- Цель атаки – установка инструментов удалённого администрирования
- ПК, к которому будут подключать ремонтируемые мобильные телефоны => полный доступ к данным

Что делать, если результат нужен быстро?
Атака на сервисные центры мобильных телефонов



- Как защититься – Content Disarm and Reconstruction
- Удаление эксплоита из вложения, мгновенная доставка письма адресату

Что делать, если результат нужен быстро?
Атака на сервисные центры мобильных телефонов

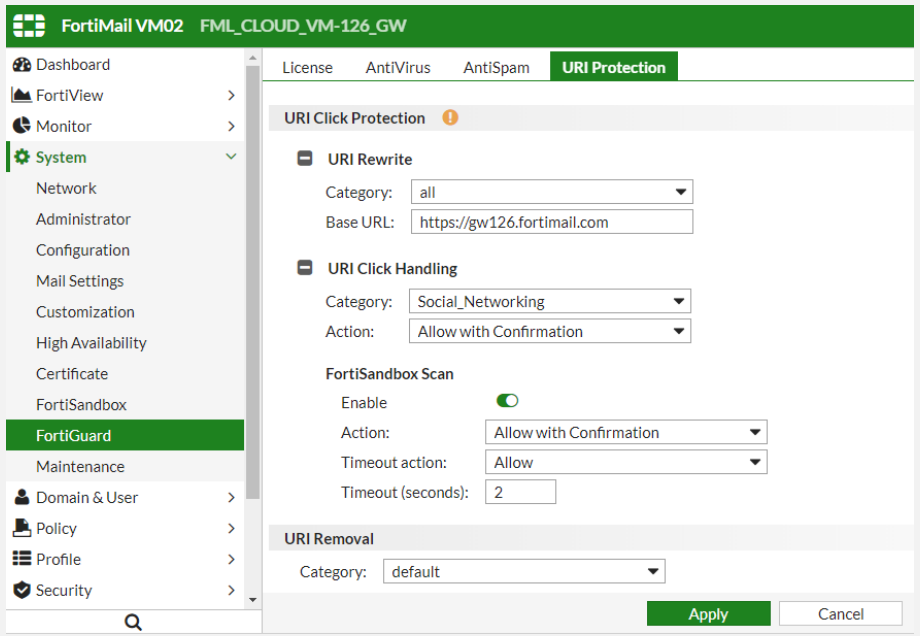


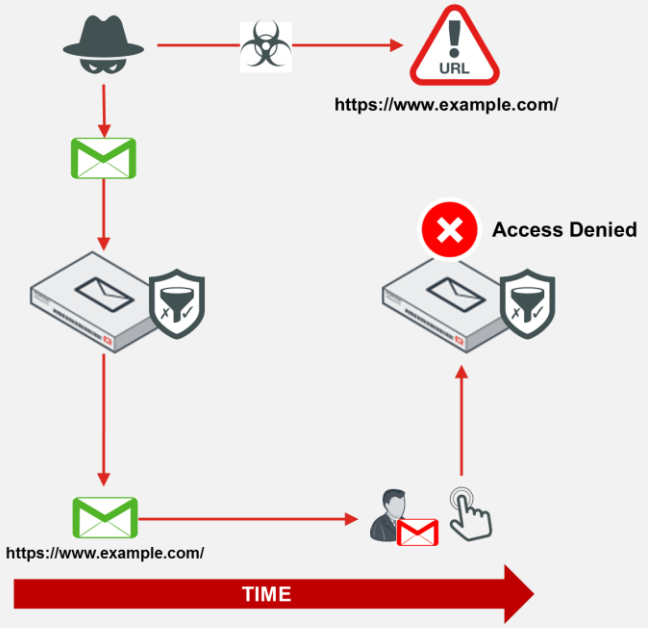
- Как защититься – Content Disarm and Reconstruction
- Удаление эксплоита из вложения, мгновенная доставка письма адресату

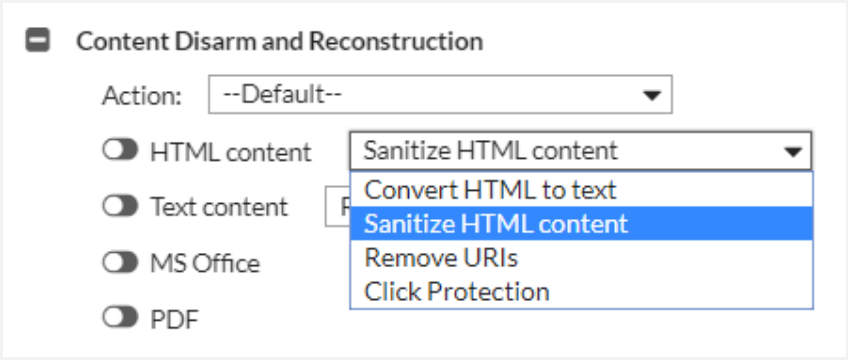
Как фильтровать ссылки и невредоносный контент?

URI Click Protection

- Защита в момент клика
  - » При проверке письма ссылки переписываются так, что они указывают на специальный портал на FortiMail
  - » При попадании пользователя по такой ссылке, FortiMail проводит повторный анализ конечной ссылки
  - » Требует лицензии URL Click Protect License (см. слайд по лицензированию)
- Преимущества
  - » Позволяет защитить пользователей от перехода по ссылкам, по которым уже после прохождения письма стал доступен вредоносный контент



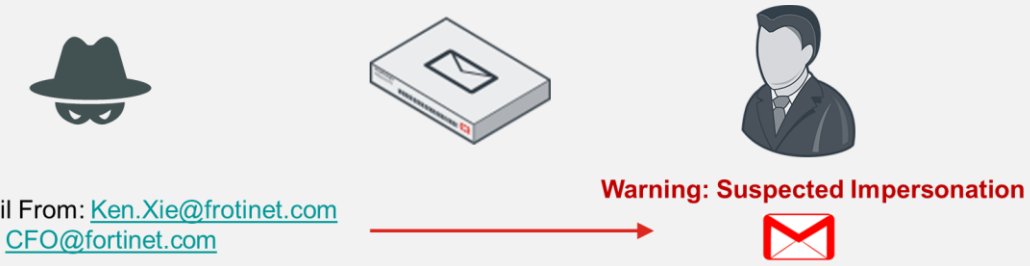


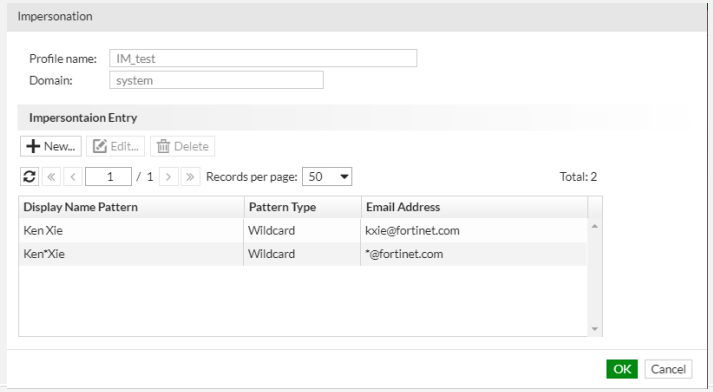


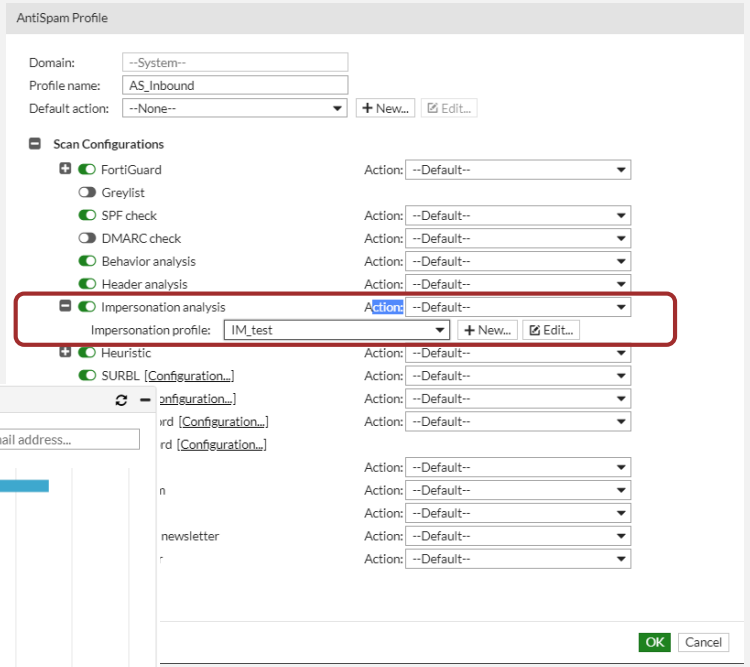
Как фильтровать ссылки и невредоносный контент?

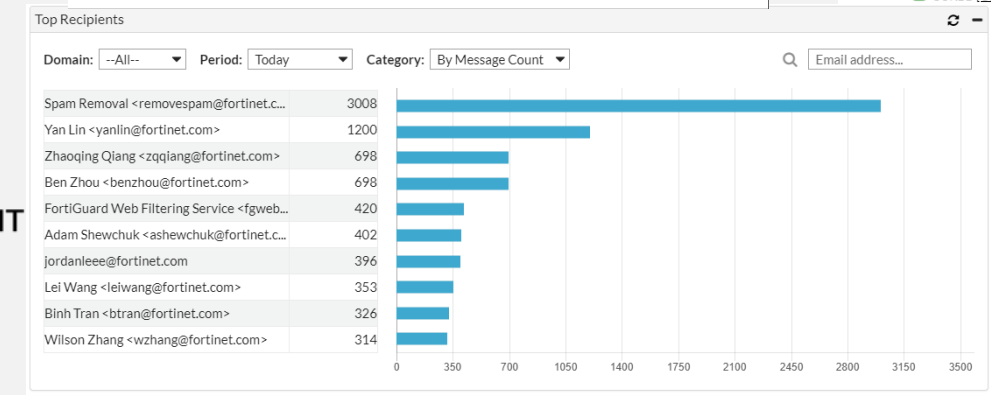
Impostor Protection

- Анализ подмены отправителя
  - » Автоматическая идентификация корректных пар отображаемого имени и адреса отправителя.
  - » Детектирование спуфинга внутренних отправителей во входящей почте и предупреждение получателей
- Преимущества
  - » Позволяет защитить от атак, основанных на социальной инженерии (например, от имени руководителя компании приходит просьба о переводе денег)
  - » Защита от BEC



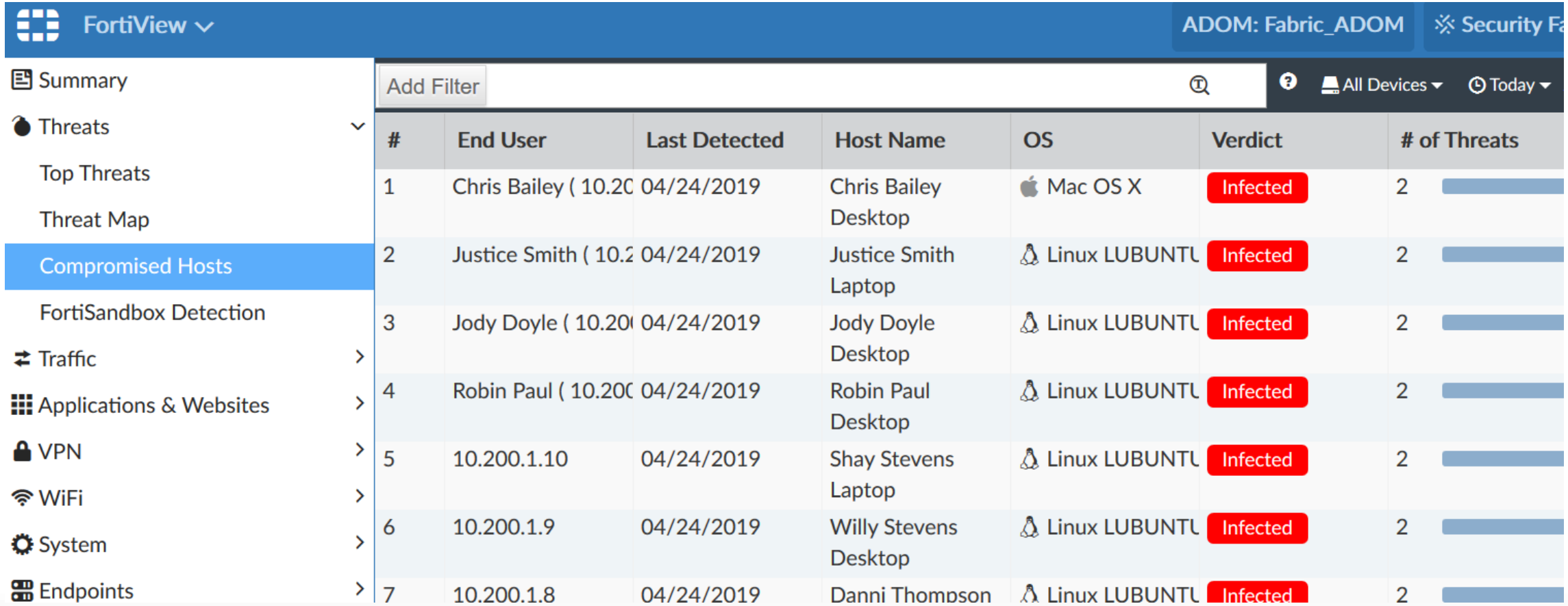






Не удалось предотвратить? Выявление компрометации

FortiAnalyzer: Indicators of Compromise (IoC)



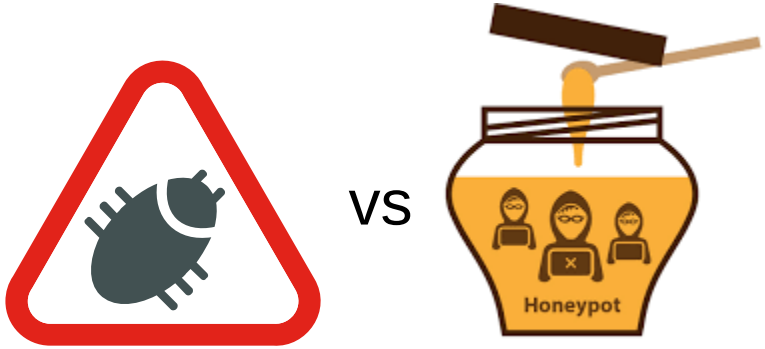
#	End User	Last Detected	Host Name	OS	Verdict	# of Threats
1	Chris Bailey (10.20	04/24/2019	Chris Bailey Desktop	Mac OS X	Infected	2
2	Justice Smith (10.2	04/24/2019	Justice Smith Laptop	Linux LUBUNTU	Infected	2
3	Jody Doyle (10.200	04/24/2019	Jody Doyle Desktop	Linux LUBUNTU	Infected	2
4	Robin Paul (10.200	04/24/2019	Robin Paul Desktop	Linux LUBUNTU	Infected	2
5	10.200.1.10	04/24/2019	Shay Stevens Laptop	Linux LUBUNTU	Infected	2
6	10.200.1.9	04/24/2019	Willy Stevens Desktop	Linux LUBUNTU	Infected	2
7	10.200.1.8	04/24/2019	Danni Thompson	Linux LUBUNTU	Infected	2

Не удалось предотвратить? Выявление компрометации

Как это улучшить?

Естественный мир

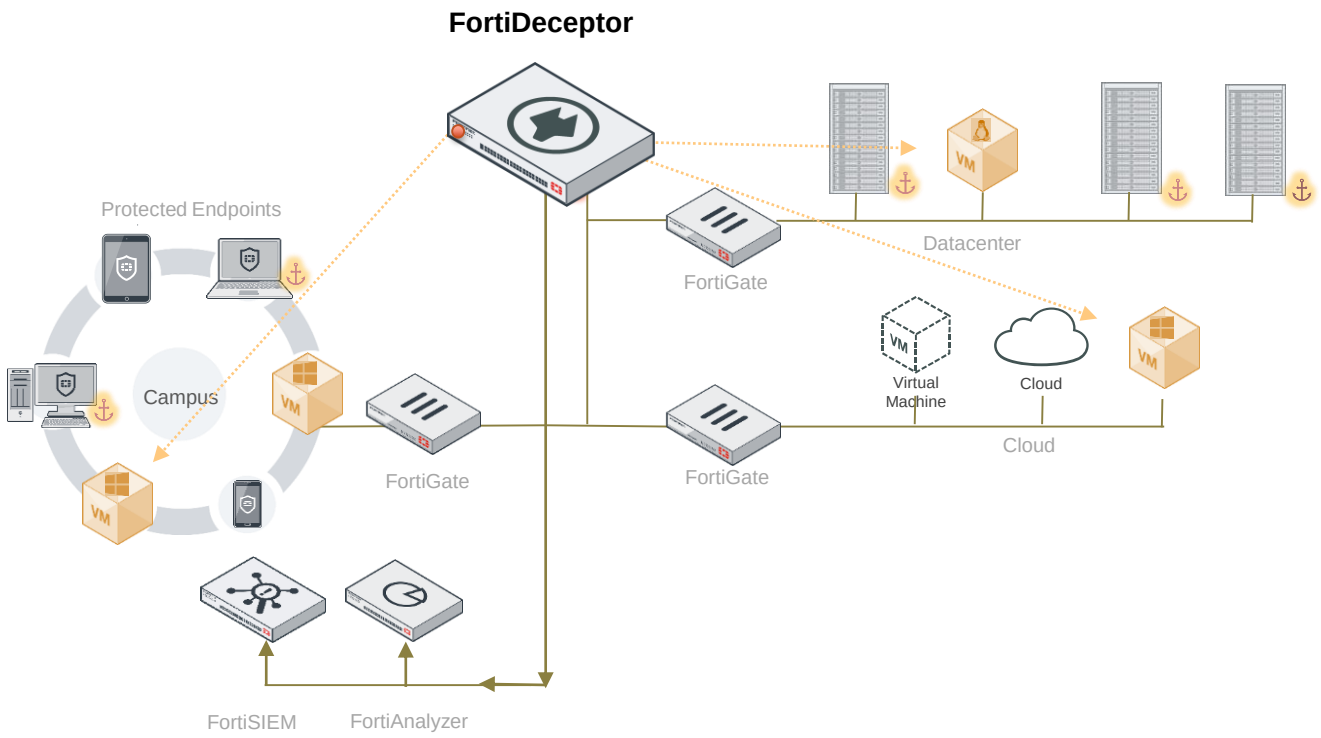
Человеческая деятельность



Киберпространство (bots vs honeypots)

Не удалось предотвратить? Выявление компрометации

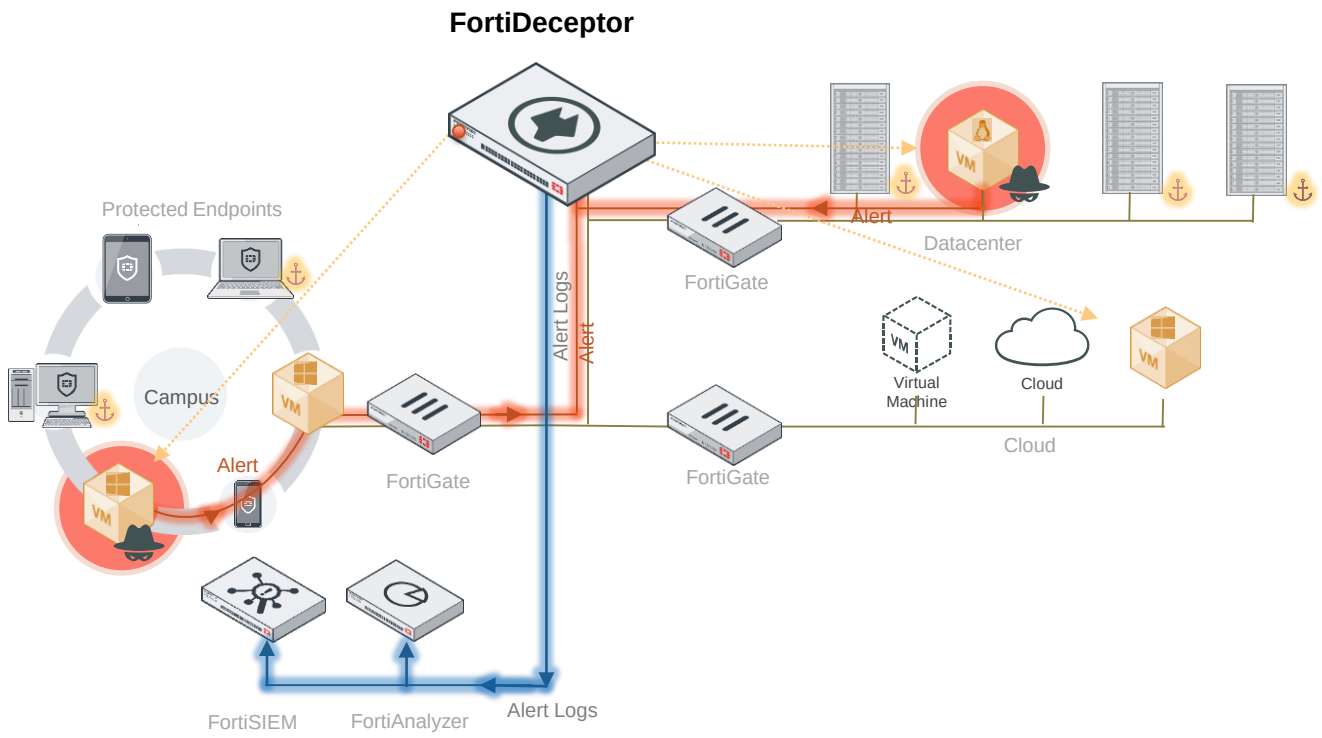
FortiDeceptor: Жизненный цикл
Обман



- Автоматическое развертывание ВМ и приманок (данных, приложений, сервисов)
- Направление атак на ВМ с конфигурацией обычных IT систем

Не удалось предотвратить? Выявление компрометации

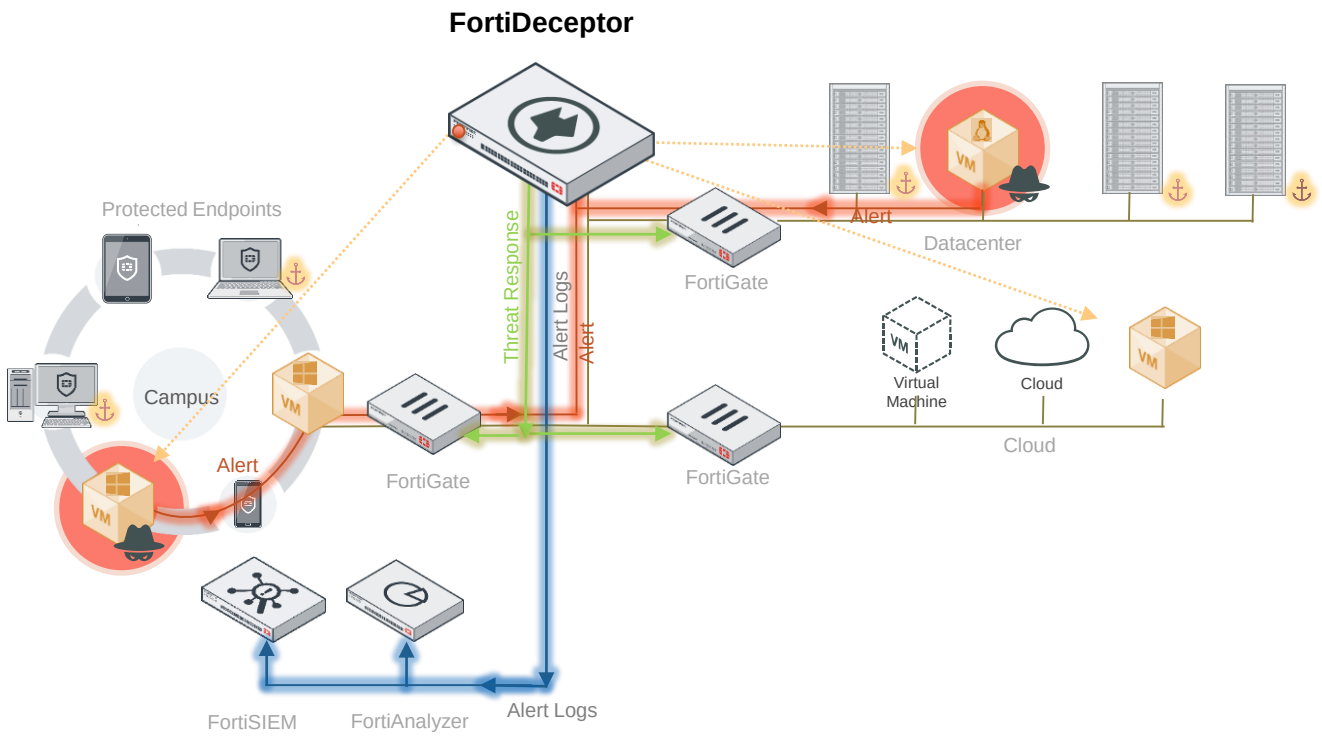
FortiDeceptor: Жизненный цикл
Обман > Уличение



- Уличение – фиксация всех действий злоумышленников в ВМ
- Корреляция событий и консолидация всех активностей в единую кампанию

Не удалось предотвратить? Выявление компрометации

FortiDeceptor: Жизненный цикл
Обман > Уличение > Устранение



- Создание индикаторов атаки – данных, по которым можно выявить скомпрометированные узлы
- Ручное и автоматическое подавление атаки – блокировка индикаторов в СЗИ

Заключение

- Атаки с применением электронной почты эффективны и наносят значительный ущерб
- Устаревшие антиспам решения не справляются и создают ложное чувство защищенности
- Fortinet ATP Framework – комбинация современных и активно развиваемых средств защиты
- Fortinet соответствует актуальным рекомендациям Gartner (Market Guide for SEG)
- **Противостоять продвинутым угрозам возможно – с продвинутым средством защиты**


FORTINET