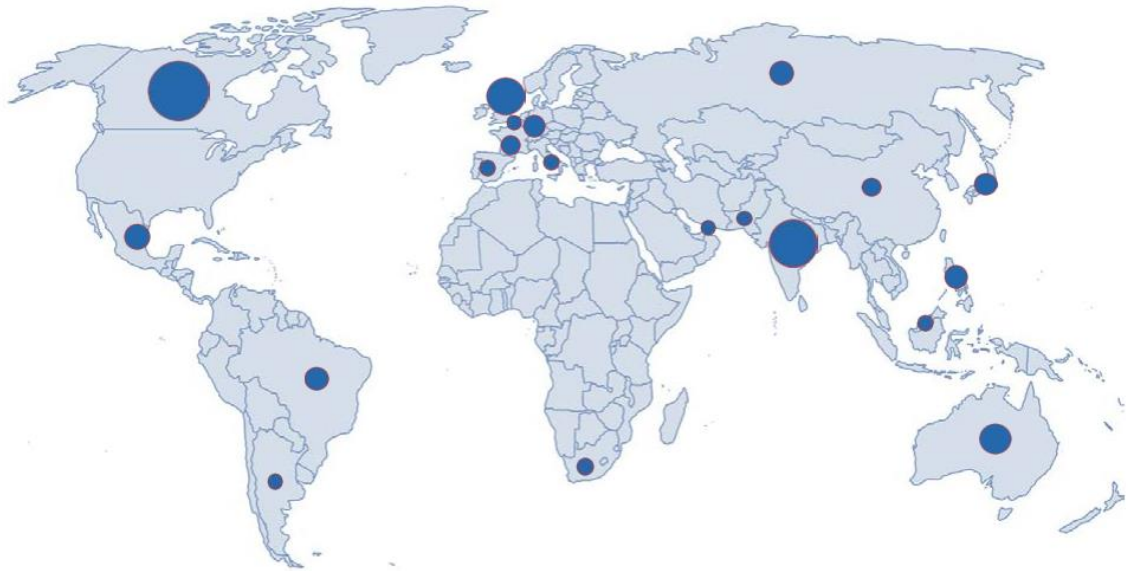
Практическая демонстрация возможностей противостояния современным угрозам

Что и зачем нужно делать? 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

Нужно защитить электронную почту от новых угроз
«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/

То есть антиспам не работает? 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

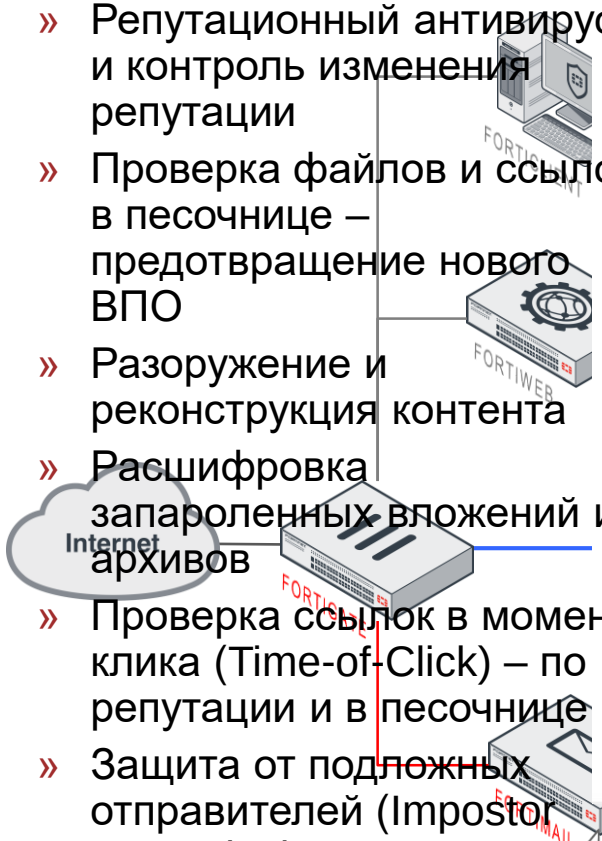
Gartner

Архитектура современного шлюза электронной почты, позволяющая противостоять продвинутым угрозам

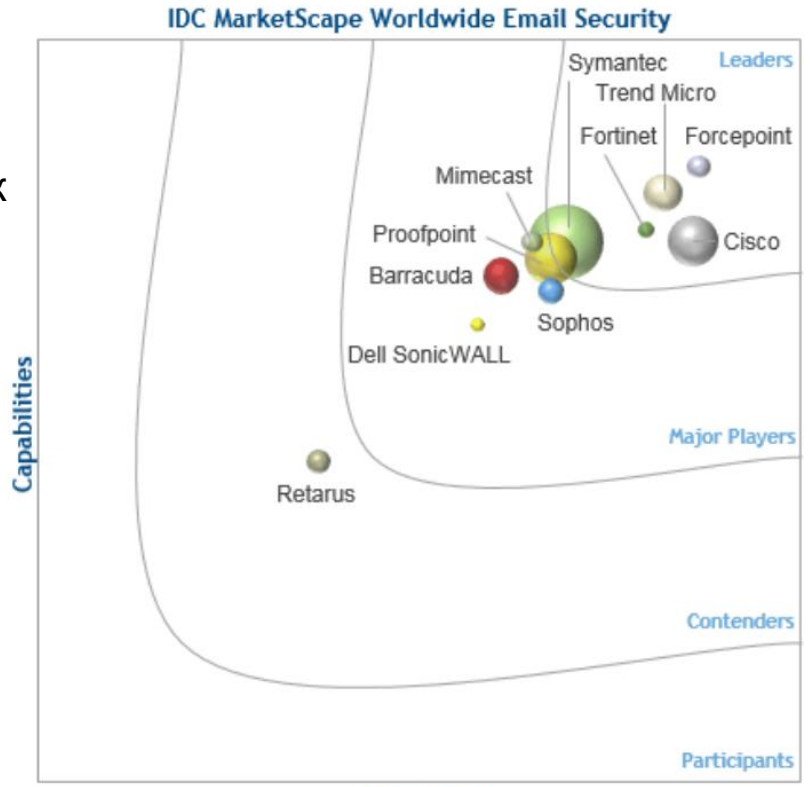
Fortinet Advanced Threat Protection – защита от продвинутых угроз

- 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*



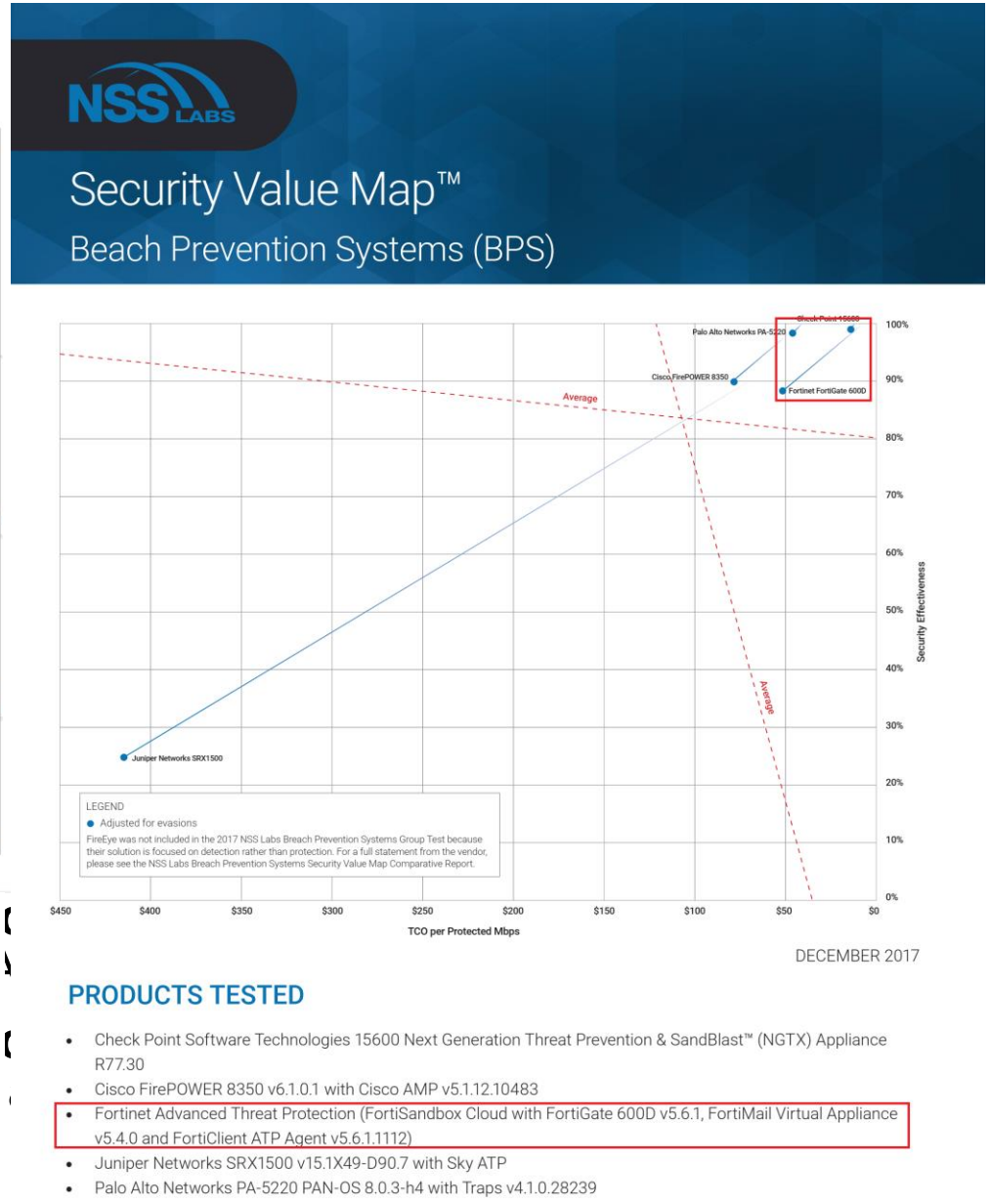
1. ПРЕД-ФИЛЬТРАЦИЯ БЛОКИРОВКА СОВРЕМЕННЫХ И РАНЕЕ НЕ ВСТРЕЧАВШИХСЯ УГРОЗ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ



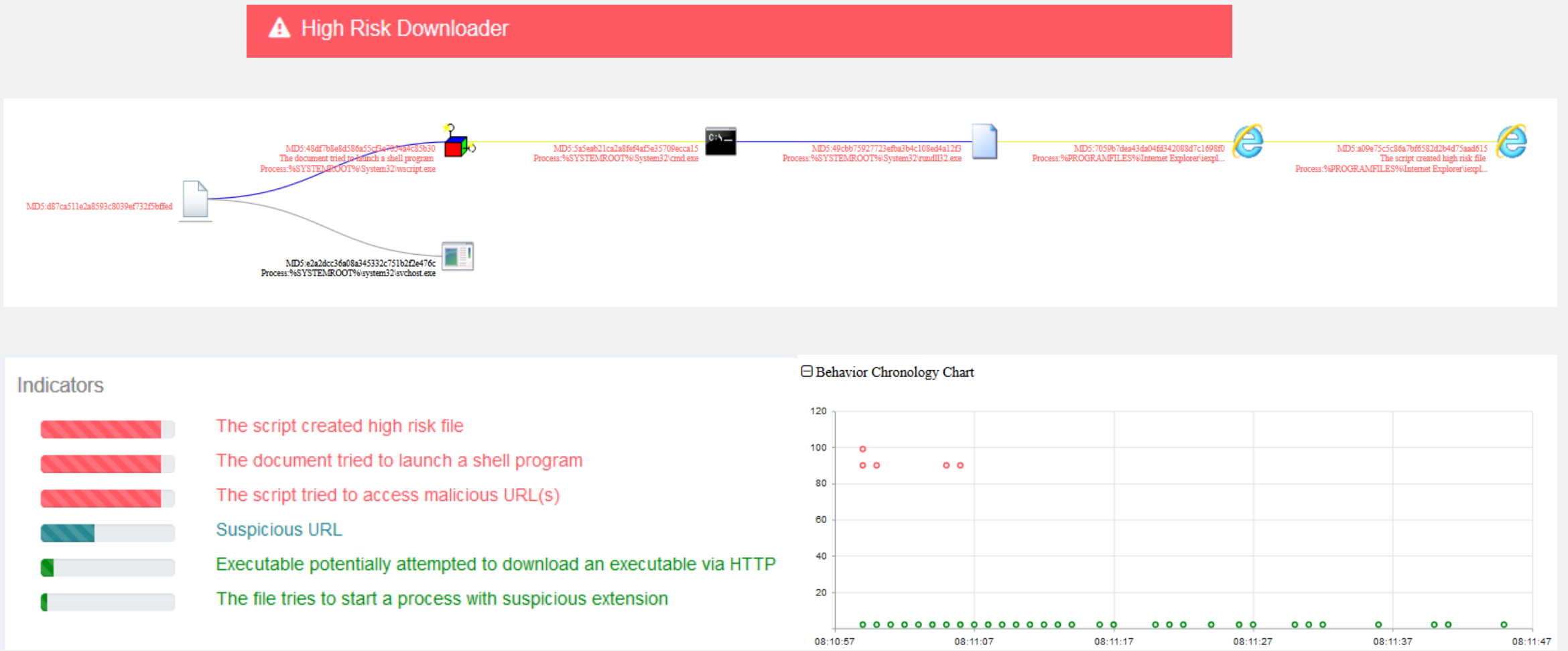
ATD-Email

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE – EMAIL

vb VERIFIED SPAM + virusbtn.com

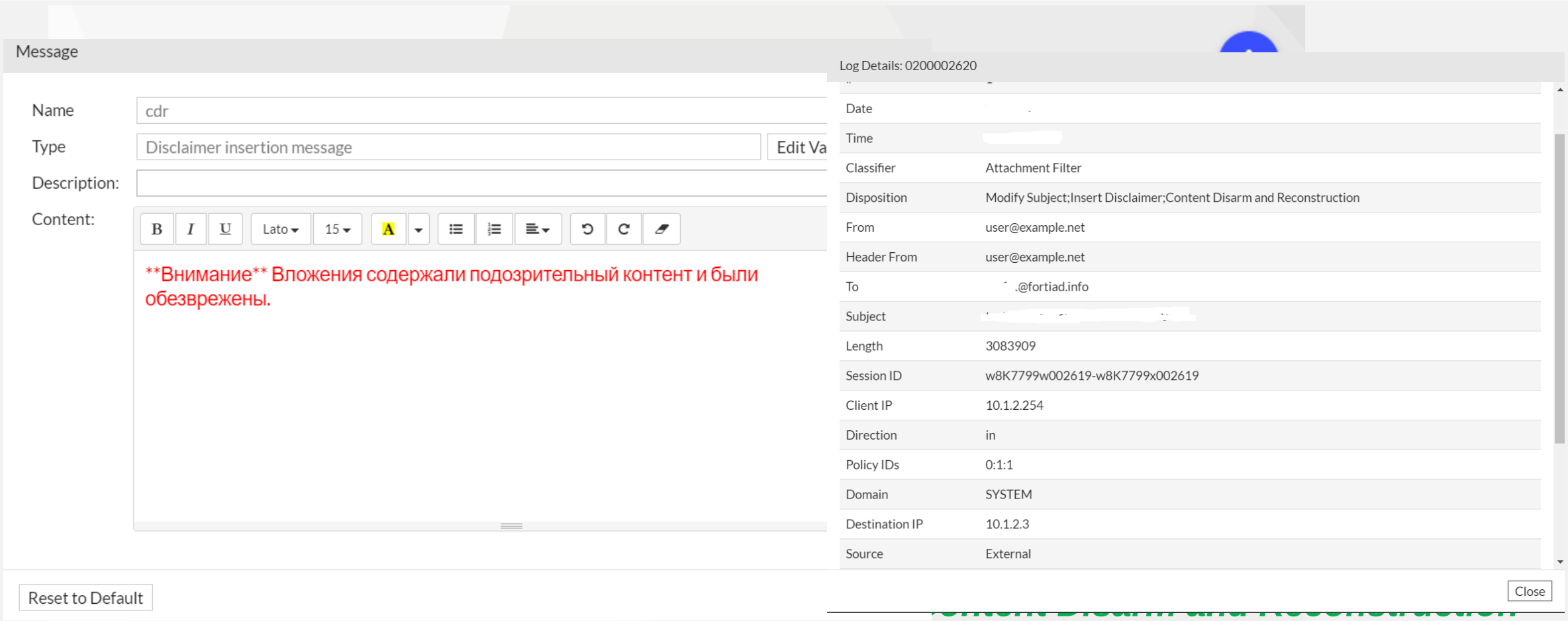


Длительная международная кампания - GandCrab



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

Локальная кампания – атака на сервисные центры по ремонту мобильных телефонов в России (07.06.2018)

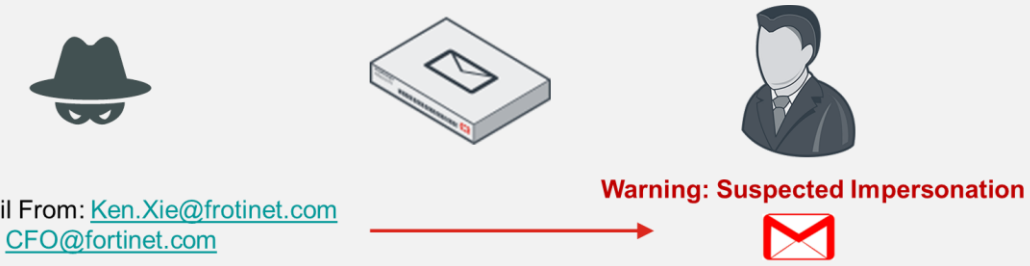


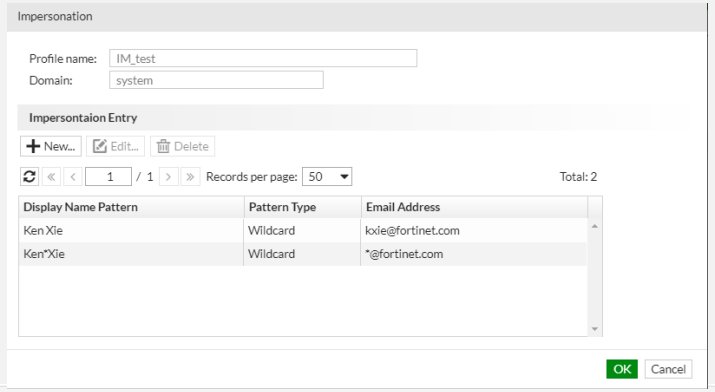
- Как защититься – Content Disarm and Reconstruction
- Удаление эксплоита из вложения, мгновенная доставка письма адресату

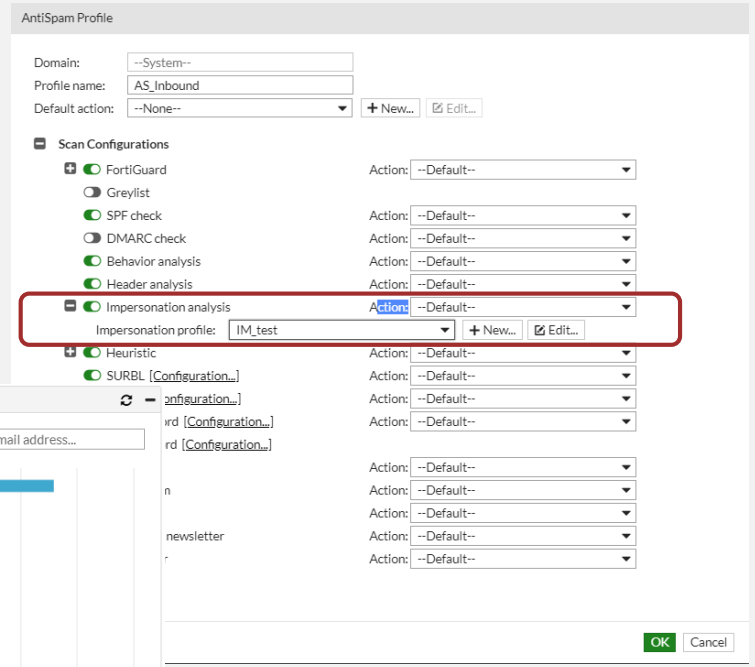
Другие возможности – URL Click Protect и Impostor Proteciton

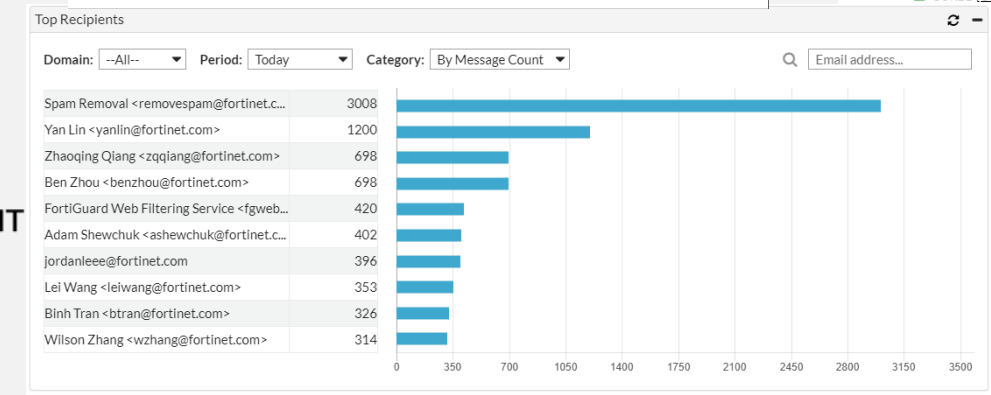
Impostor Protection

- 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









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®