

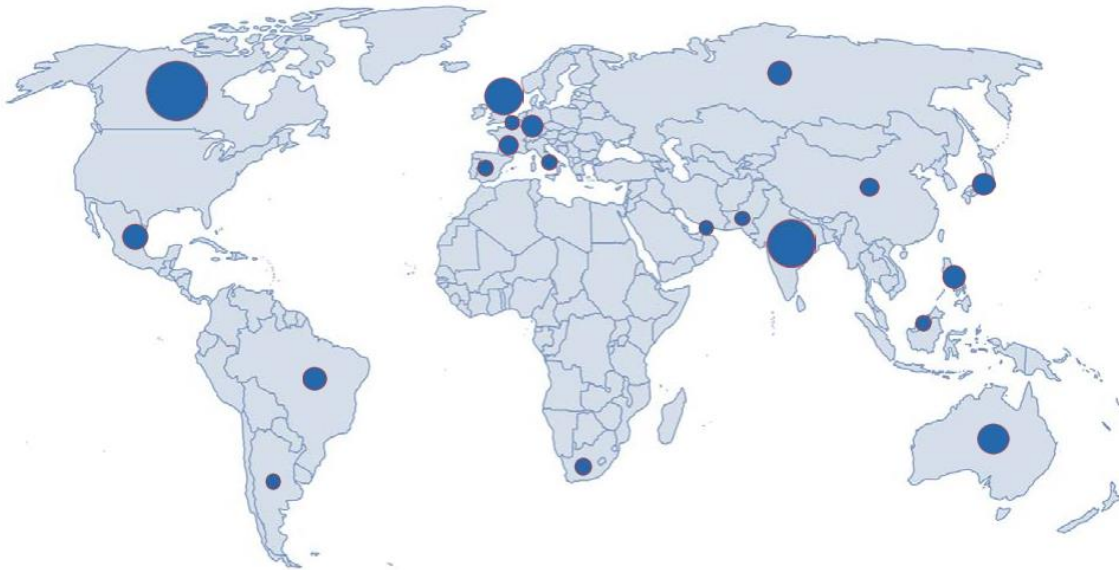
Практическая демонстрация возможностей противостояния современным угрозам

Что и зачем нужно делать? Cyber Threat Intelligence

FBI IC2 - 2017 Internet Crime Report

Top 20 Foreign Countries by Victim

Excluding the United States¹⁷



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

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.

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

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	Hactivist	\$20,147
Lottery/Sweepstakes	\$16,835,001	Terrorism	\$18,926
Extortion	\$15,302,792	No Lead Value	\$0
Tech Support	\$14,810,080		

Social Media \$56,478,483
Virtual Currency \$58,391,810

*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.

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?

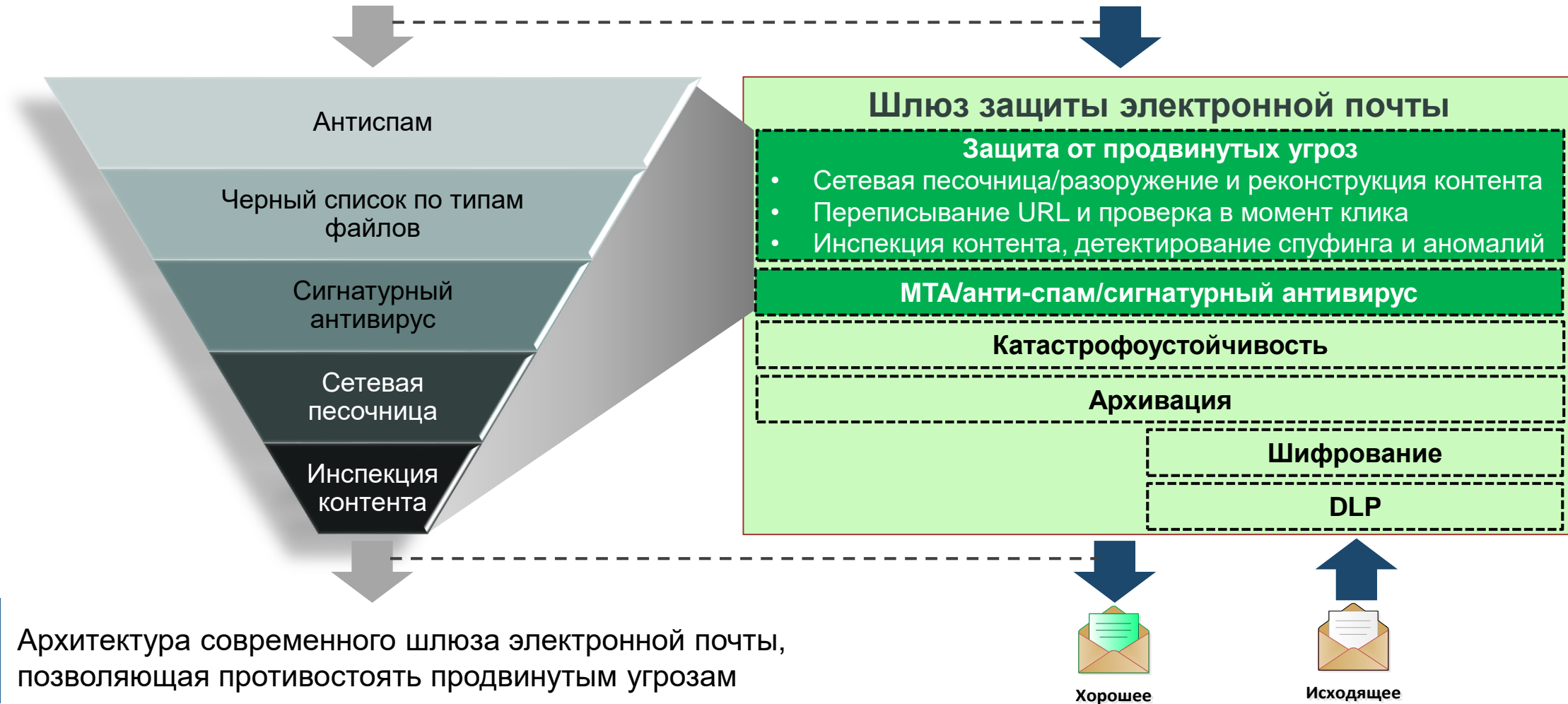
Gartner - Market Guide for Secure Email Gateways

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

Продвинутые угрозы

- С вложениями
- Со ссылками
- Подложный отправитель

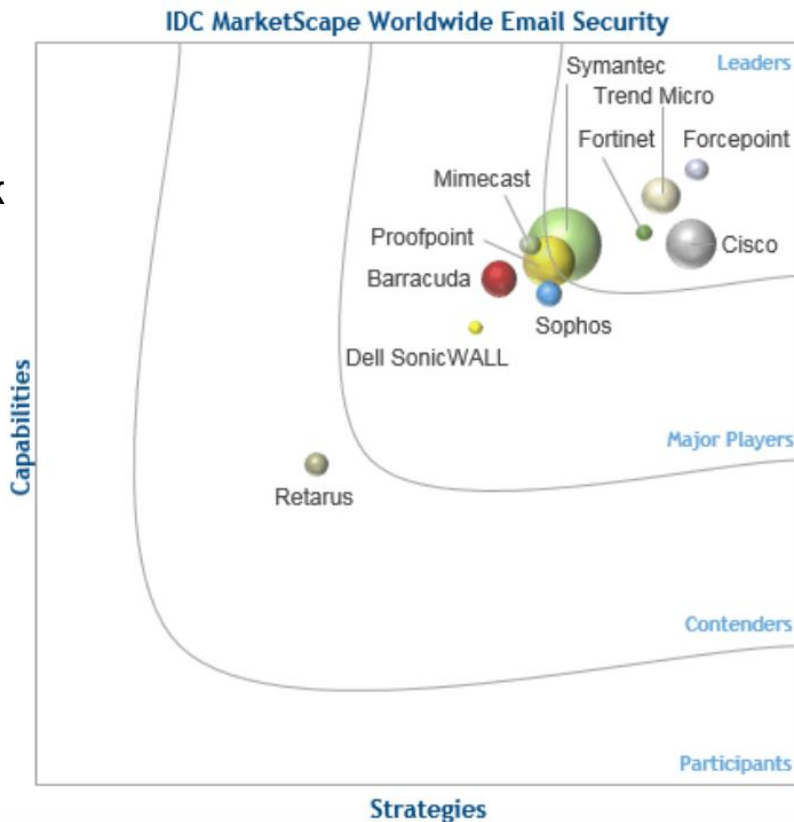
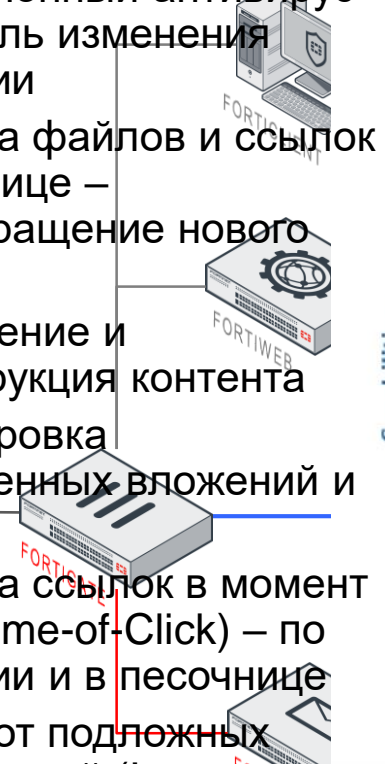
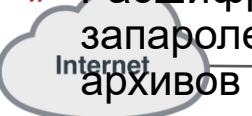
Спам Хорошее Плохое



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)



★ **ATD-Email**

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE - EMAIL

vb VERIFIED SPAM + virusbtn.com

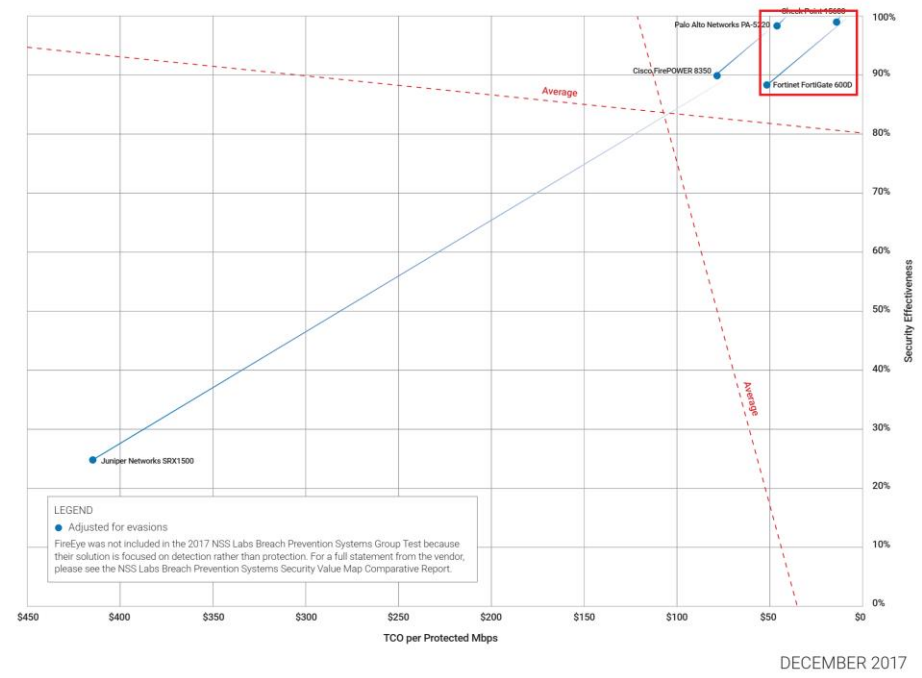
» И это далеко не всё

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

NSS LABS

Security Value Map™

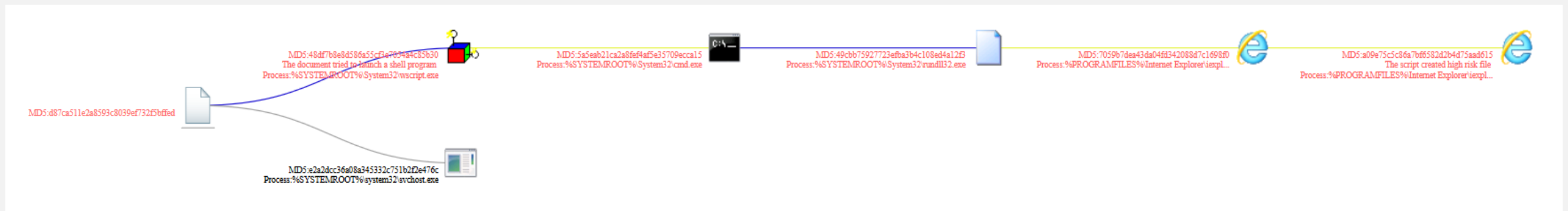
Beach Prevention Systems (BPS)



- 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

Длительная международная кампания - GandCrab

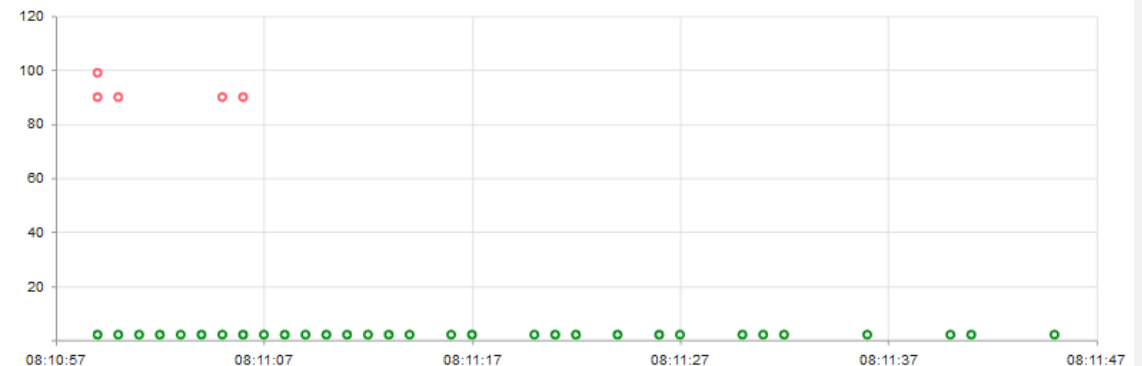
High Risk Downloader



Indicators

- The script created high risk file
- The document tried to launch a shell program
- The script tried to access malicious URL(s)
- Suspicious URL
- Executable potentially attempted to download an executable via HTTP
- The file tries to start a process with suspicious extension

Behavior Chronology Chart



- 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)

Message

Name: cdr

Type: Disclaimer insertion message Edit Va

Description:

Content:

****Внимание** Вложения содержали подозрительный контент и были обезврежены.**

Log Details: 0200002620

Date	
Time	
Classifier	Attachment Filter
Disposition	Modify Subject;Insert Disclaimer;Content Disarm and Reconstruction
From	user@example.net
Header From	user@example.net
To	...@fortiad.info
Subject	
Length	3083909
Session ID	w8K7799w002619-w8K7799x002619
Client IP	10.1.2.254
Direction	in
Policy IDs	0:1:1
Domain	SYSTEM
Destination IP	10.1.2.3
Source	External

Reset to Default Close

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

Другие возможности – URL Click Protect и Impostor Protection

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

Mail From: Ken.Xie@frotinet.com
To: CFO@fortinet.com

Warning: Suspected Impersonation

Impersonation

Profile name: IM_test
Domain: system

Impersonation Entry

Display Name	Pattern	Pattern Type	Email Address
Ken Xie	Ken Xie	Wildcard	kxie@fortinet.com
Ken Xie	Ken Xie	Wildcard	*@fortinet.com

AntiSpam Profile

Domain: --System--
Profile name: AS_Inbound
Default action: --None--

Scan Configurations

- FortiGuard Action: --Default--
- Greylist Action: --Default--
- SPF check Action: --Default--
- DMARC check Action: --Default--
- Behavior analysis Action: --Default--
- Header analysis Action: --Default--
- Impersonation analysis Action: --Default--**
Impersonation profile: IM_test
- Heuristic Action: --Default--
- SURBL [Configuration...] Action: --Default--

Top Recipients

Domain	Period	Category	Count
Spam Removal <removespam@fortinet.c...>	Today	By Message Count	3008
Yan Lin <yanlin@fortinet.com>			1200
Zhaoqing Qiang <zqiang@fortinet.com>			698
Ben Zhou <benzhou@fortinet.com>			698
FortiGuard Web Filtering Service <fgweb...>			420
Adam Shewchuk <ashewchuk@fortinet.c...>			402
jordanlee@fortinet.com			396
Lei Wang <leiwang@fortinet.com>			353
Binh Tran <btran@fortinet.com>			326
Wilson Zhang <wzhang@fortinet.com>			314

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**

The logo for FERTINET is displayed in a bold, white, sans-serif font. The letter 'F' is stylized with three horizontal bars. The letters 'E', 'R', 'T', 'I', 'N', and 'E' are solid. The final 'T' is also solid. A registered trademark symbol (®) is located to the right of the final 'T'. The background is a solid blue color with a complex, white, isometric wireframe pattern of overlapping rectangular and cubic shapes, creating a sense of depth and architectural structure.

FERTINET®