Экспертные данные АО «ПМ». Анонс нового продукта

Артём Савчук,
заместитель технического директора,
«Перспективный мониторинг»

АО «ПМ» сегодня

12

лет на рынке услуг SOC и исследования защищённости

7

лет центр ГосСОПКА (А)

>1600

выполненных ИБ проектов

13

действующих киберполигонов Ampire

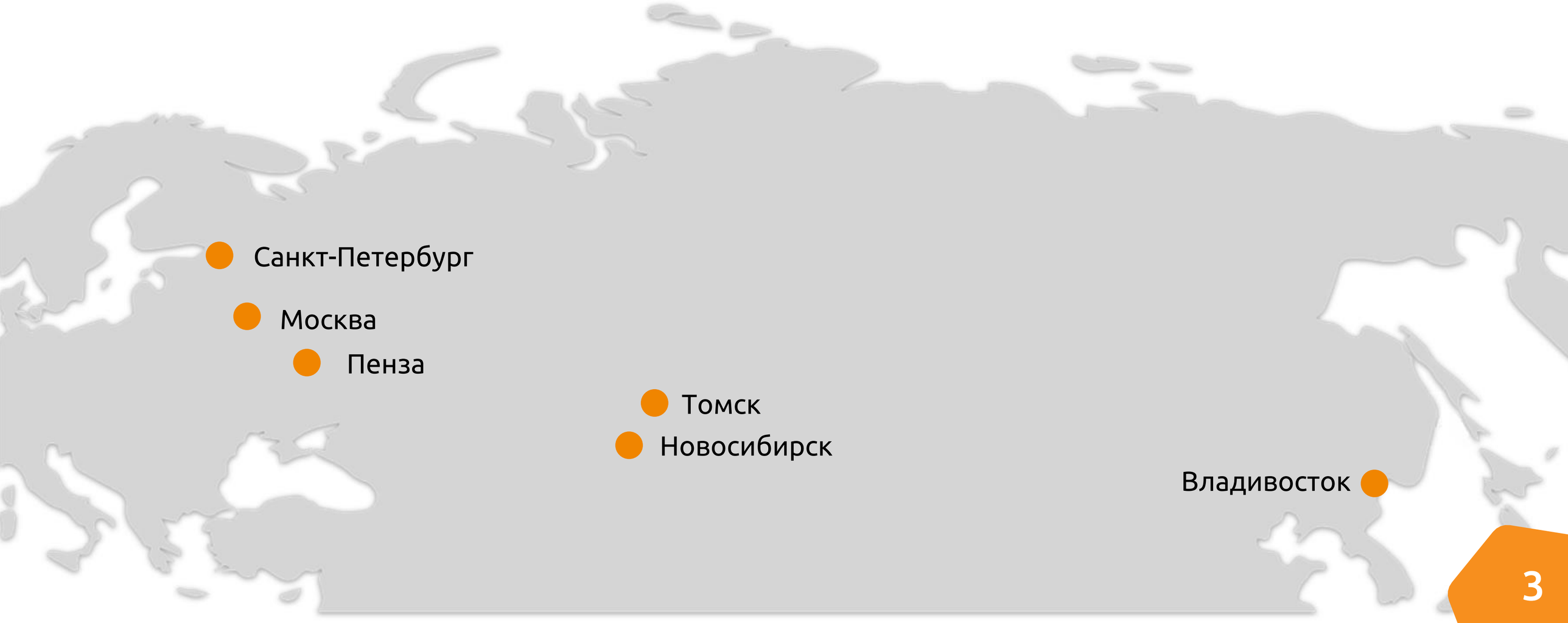
300+

проведенных киберучений

3000+

ИБ специалистов прошли обучение на Ampire

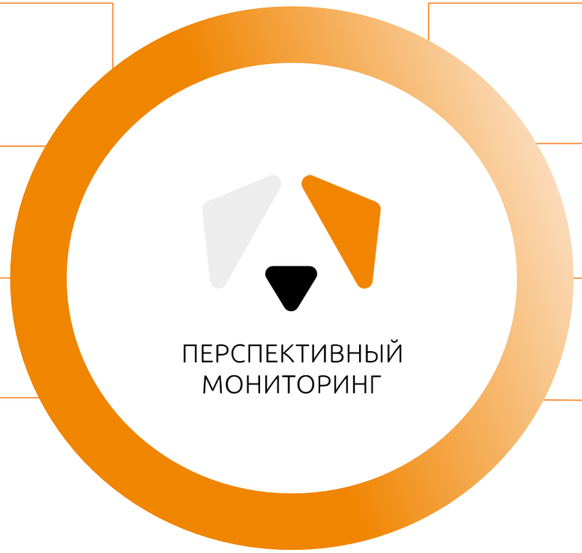
Регионы присутствия



Направления деятельности

Исследование защищённости

- Пентест
- Аудит ИБ
- Оценка соответствия требованиям Банка России
- Категорирование объектов КИИ



SOC

- Коммерческий SOC
- Подключение к ГосСОПКА
- Расследование инцидентов ИБ
- Группа быстрого реагирования

Продукты

- Экспертные данные
- БРП AM Rules
- AM Threat Intelligence
- Киберполигон Ampire

Сквозная экспертиза по всем направлениям деятельности АО «ПМ»

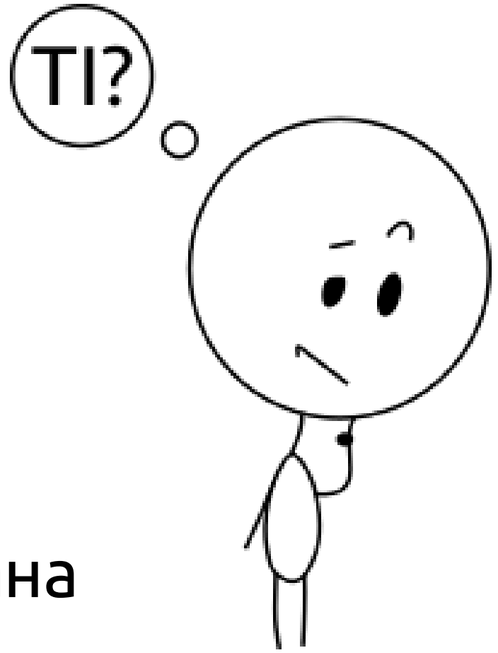
Экспертные данные
АО «ПМ»

Как кибербразведка (TI) помогает в условиях целевых атак ?

Опрос зрителей онлайн-конференции AM Live, проходившей 07 сентября 2022 года и посвящённой Threat Intelligence

Что такое и зачем нужен TI?

TI: Threat Information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes*.

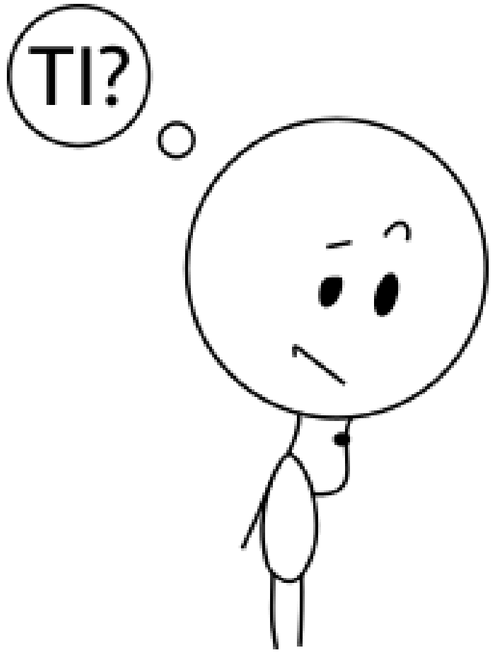


Информация об угрозах, которая была собрана, преобразована, проанализирована, интерпретирована или обогащена для обеспечения необходимого контекста для процессов принятия решений.

* https://csrc.nist.gov/glossary/term/threat_intelligence

Что такое и зачем нужен TI?

TI: The "cyclical practice" of planning, collecting, processing, analyzing and disseminating information that poses a threat to applications and systems**.



"Циклическая практика" планирования, сбора, обработки, анализа и распространения информации, содержащей сведения об угрозах для приложений и систем.

** https://en.wikipedia.org/wiki/Threat_intelligence

Как устроен процесс

Сбор

- Открытые источники
- Sandbox
- Объекты пользователей
- Ручное добавление
- Хакерские инструменты

Обработка

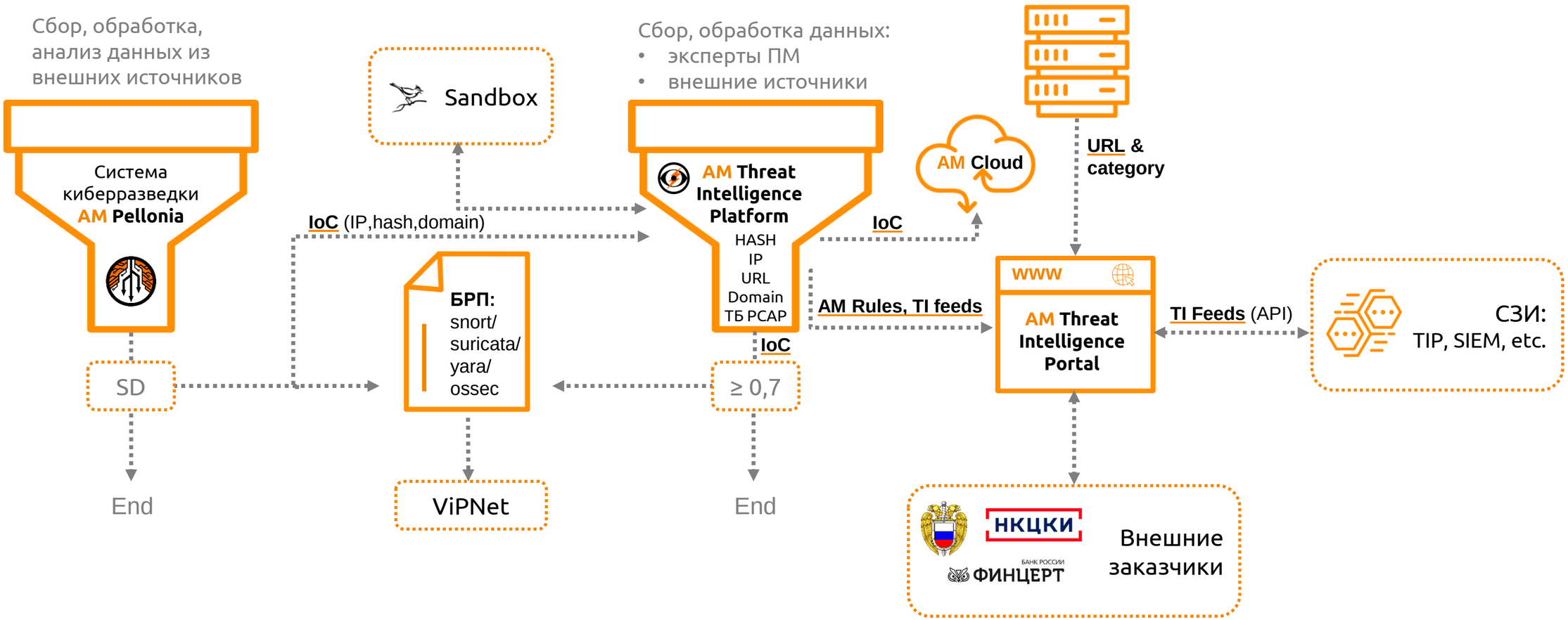
- Модели ML
- IDS/IPS (NGFW)
- Sandbox
- AV
- Парсеры
- Вспомогательные сервисы
- Тестирование

Поставка

- БРП
- AM Rules
- TI feeds (IOC)
- Бюллетени ИБ

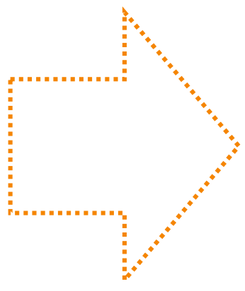
В основе наших фидов — данные об угрозах, аккумулированные экспертами АО «ПМ» в ходе расследований инцидентов и изучения деятельности хакерских группировок во всем мире, а также данные обезличенной телеметрии, полученные с инсталляций продуктов АО «ИнфоТеКС» в десятках компаний.

Как устроено



Направление исследования киберугроз

- Эксплоиты
- ВПО
- Хакерские инструменты
- Целевые атаки
- Threat Intelligence
- […]



ЭД

- БРП для продуктовой линейки ViPNet ИнфоТеКС
- AM_Rules (snort, yara, ossec, suricata rules)
- IOC
- URL Categorization
- Бюллетени

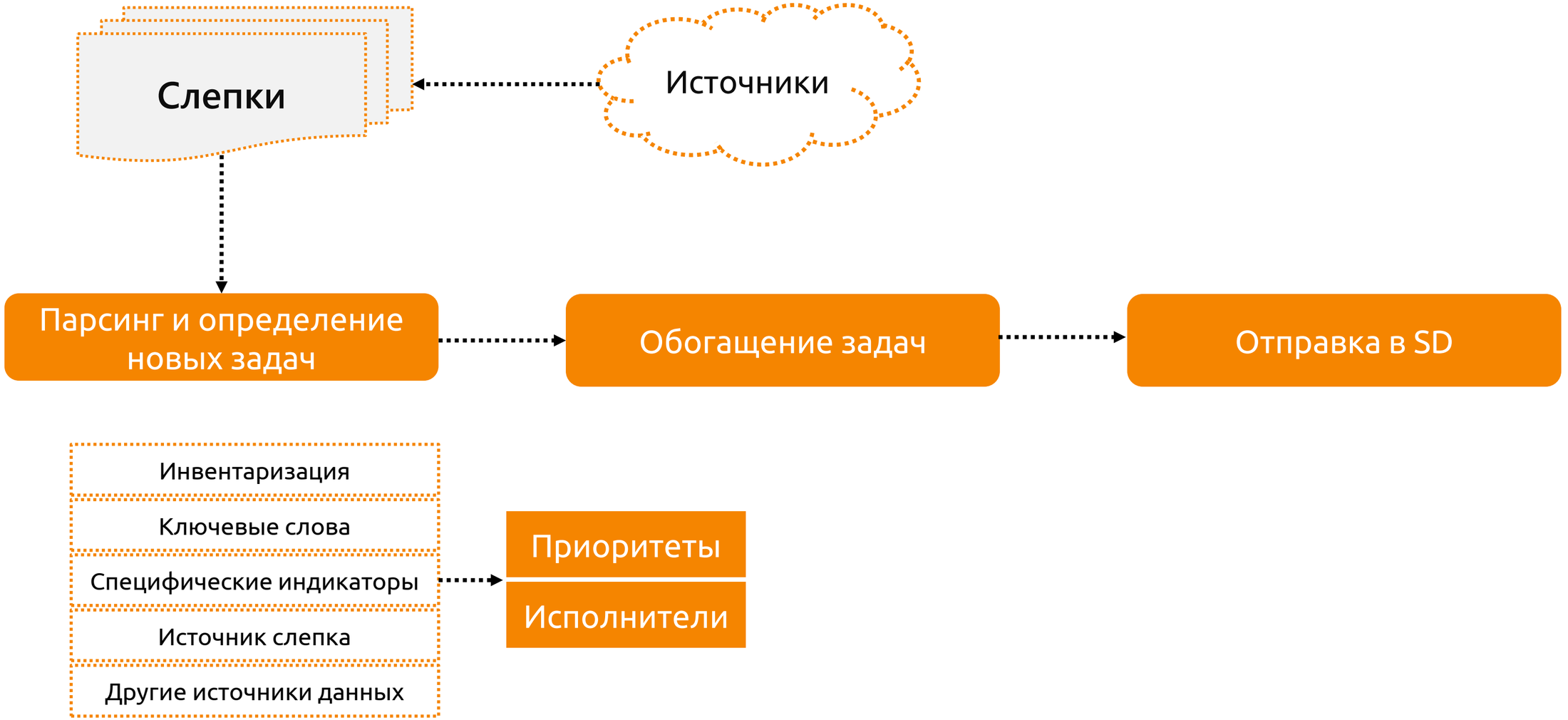
Экспертные данные
АО «ПМ»

1. «Базы решающих правил» (БРП, включают наборы snort, yara, ossec, suricata правил)
2. TI feeds (IoC в STIX или любом другом пользовательском формате)
3. AM Rules (Свидетельство Роспатента №2016620316 от 03.03.2016 г.)
4. Категорированные веб-ресурсы
5. Бюллетени ИБ

Наши источники

НКЦКИ	ФинЦЕРТ	NVD CVE	DHS CISA
Exploit-DB	Packet Storm Security	GitHub	Cisco Talos
Malware Traffic Analysis	Crowdstrike Research	Zero Day Initiative	McAfee Labs
Dr. Web	ESET WeLiveSecurity	FireEye Threat Research	Positive Technologies
TrustWave SpiderLabs	ThreatPost	HackerNews	KrebsOnSecurity
Securelist	SecLists Full Disclosure	Fortinet Threat Research	Palo Alto Unit42
SecurityFocus	Trend Micro Research	Check Point Research	и другие (>30 шт.)

Работа с публичными источниками



AM TI Platform

Вычисляем, используя следующие признаки:

- Факт того, что домен был создан автоматически (модель DGA)
- Рейтинг AV
- Количество источников feed'ов
- Мета (косвенная) информация (срабатывания правил, результаты моделей МО, «негативный контекст», добавлен аналитиком и др.)

Индикаторы компрометации (IoC)

Пирамида индикаторов компрометации в зависимости от сложности получения данных (т.н. «Пирамида боли» David J Bianco)

IPv4 | Domain | Хэши (MD5, SHA1)

URL | Транзакционные (MTA, User-agent) | Имена файлов/путь

mutex | Значения реестра | e-mails

Наиболее популярные типы индикаторов компрометации

Наложение известных индикаторов компрометации на этапы Kill Chain

*https://www.securitylab.ru/blog/personal/Business_without_danger/320988.php

Источники данных об IoC

- urlhause
  last update: 2023-08-22T12:00:00
- dshield
  last update: 2023-09-05T00:00:00
- joewein
  last update: 2021-01-15T00:00:00
- botvrij
  last update: 2020-12-29T12:48:00
- feodotracker
  last update: 2023-08-26T00:00:00
- et
  last update: 2023-09-05T00:00:00
- cinsscore
  last update: 2023-09-05T00:02:00
- openphish
  last update: 2023-09-05T00:00:00
- darklist_de
  last update: 2023-08-12T00:00:00
- blackbook
  last update: 2023-08-21T03:00:00
- greensnow
  last update: 2023-09-05T03:00:00
- nocoin
  last update: 2023-04-13T00:00:00

- inquest
  last update: 2023-09-05T03:00:00
- cybercrime
  last update: 2023-07-04T03:00:00
- binarydefense
  last update: 2023-04-19T03:00:00
- threatfox
  last update: 2023-09-05T03:00:00
- digitalside
  last update: 2023-09-05T04:00:00
- malwarehosts
  last update: 2023-08-22T05:44:00
- blocklistde
  last update: 2023-09-05T06:55:00

Stix/Taxii Parser

- stix-anomali
  last update: 2023-09-01T01:02:00
- stix-alienvault
  last update: 2023-09-01T01:02:00

Automatically added

- hybrid
- bazaar
- malshare
- virusshare
- joesandbox
- tria

«Система киберразведки AM Pellonia»
Свидетельство о государственной регистрации программы для ЭВМ №2023666988

Статистика IoC

Периодичность	IP	Domain	Hash	URL	Samples
В день ~	3 400	2 100	1 700	41 200	1 160
В неделю ~	24 100	15 400	12 300	289 700	8 150
В месяц ~	96 000	61 700	49 300	1 158 900	32 600
		> 1 900 000 samples pcap			
TOTAL		>100 196 000 IP, domain, url, hash, samples			

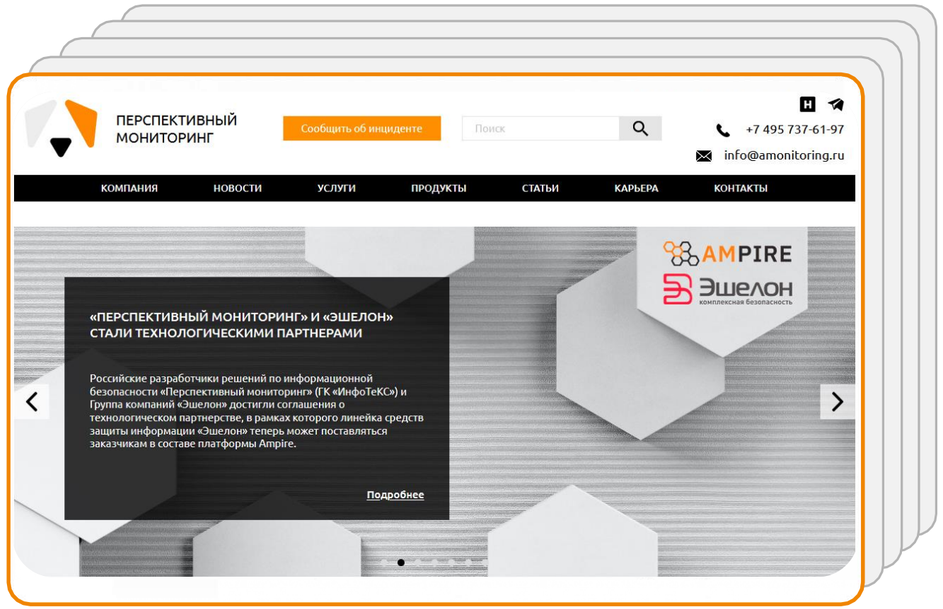
Система БРП

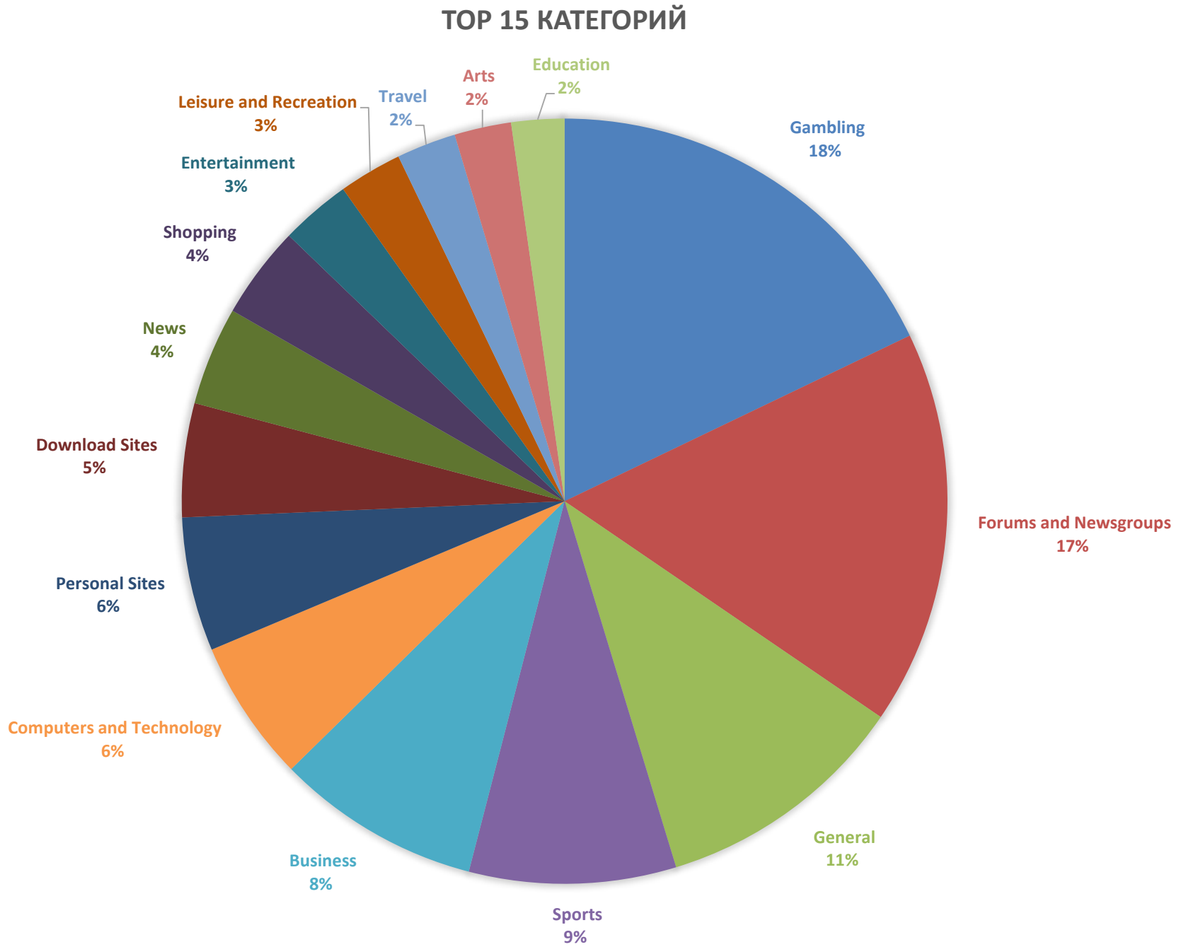
Дата изменения	Группа	SID	Сообщение
15.09.23 11:28	emerging-exploit	3243759	ET EXPLOIT TP-Link Archer AX21 < v1.1.4 Unauthenticated Command Injection (CVE-2023-1389)
14.09.23 16:39	emerging-exploit	3243758	AM EXPLOIT Tenda AC5 <= v15.03.06.28 RCE (CVE-2023-31587)
16.09.23 15:04	emerging-shellcode	3243589	AM SHELLCODE BSDi x86 Bind Shell MSF variant (UDP)
06.09.23 15:23	emerging-trojan	3243588	ET TROJAN (ANY.RUN) Echida Botnet Check-In M2
06.09.23 15:23	emerging-trojan	3243587	ET TROJAN (ANY.RUN) Echida Botnet Check-In M1
16.09.23 15:04	emerging-shellcode	3243586	AM SHELLCODE BSDi x86 Bind Shell MSF variant (TCP)
05.09.23 15:19	emerging-exploit	3243584	AM EXPLOIT Possible Juniper JunOS EX/SRX series v20.4 - v22.4 RCE (CVE-2023-36845)
05.09.23 15:17	emerging-exploit	3243583	AM EXPLOIT Juniper JunOS EX/SRX series v20.4 - v22.4 Arbitrary File Upload (CVE-2023-36846)
07.09.23 11:57	emerging-exploit	3243582	AM EXPLOIT D-Link DIR-823G <= v.1.02B05 Buffer Overflow (CVE-2023-26612, CVE-2023-26616)
11.09.23 14:53	emerging-exploit	3243410	AM EXPLOIT Possible WordPress NinjaForms Plugin < v3.6.26 Reflected XSS (CVE-2023-37979)
01.09.23 11:37	emerging-trojan	3243409	AM TROJAN UNC4841 M_Backdoor_SEASPY_TfuZ Activity
01.09.23 10:47	emerging-trojan	3243408	AM TROJAN UNC4841 M_Backdoor_SEASPY_oXmp Activity
07.09.23 11:18	emerging-exploit	3243407	AM EXPLOIT Possible Perl::HTML-StripScripts <= v1.06 ReDoS (CVE-2023-24038)
16.09.23 15:04	emerging-exploit	3243406	AM EXPLOIT Possible drachtio-server < v0.8.20 DoS (CVE-2022-47516)
31.08.23 15:23	emerging-trojan	3243400	ET TROJAN (ANY.RUN) TheBoxClipper (updatebildchange)
31.08.23 15:23	emerging-trojan	3243399	ET TROJAN (ANY.RUN) TheBoxClipper CnC Activity (getkeys)
31.08.23 15:23	emerging-trojan	3243398	ET TROJAN (ANY.RUN) TheBoxClipper (addbild)
16.09.23 15:04	emerging-info	3243396	ET INFO Lets Encrypt Free SSL Cert Observed with IDN/Punycode Domain - Possible Phishing
16.09.23 15:04	emerging-exploit	3243395	AM EXPLOIT Possible Sofia-SIP < v1.13.8 Out-Of-Bounds Read (CVE-2022-31002)
16.09.23 15:04	emerging-exploit	3243394	AM EXPLOIT Possible Sofia-SIP < v1.13.8 Out-Of-Bounds Write (CVE-2022-31003)

Система БРП («Баз решающих правил») автоматизирует выпуск сборок БРП для различных продуктов АО «ИнфоТеКС»

URL-фильтрация

- 81 категория
- > 43 млн. доменов





Бюллетени ИБ

Информационный бюллетень Центра мониторинга АО «ПМ»

Название документа	**Уязвимости в Google Chrome**
Разослан	2022-10-13
Идентификатор	AM-2022-ALE-1013-02
Описание угроз	**CVE-2022-1309**

CVSSv3: 9.6, CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Объект уязвимости: Реализация DevTools API для Google Chrome

Требования к атакующему: Удаленный неаутентифицированный

Максимальный результат атаки: Исполнение произвольного кода

Бюллетени ИБ

Меры противодействия

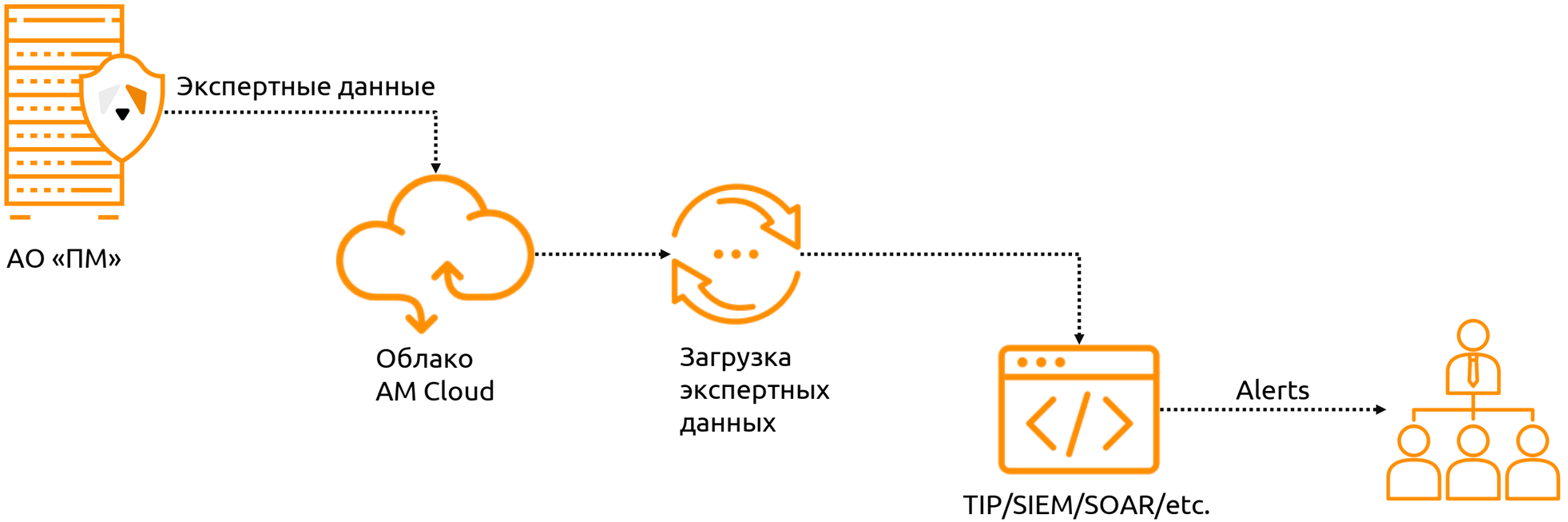
Точечно установить новую версию или комплексно обновиться до последних версий, проверив обновления на совместимость

Использовать правила ViPNet

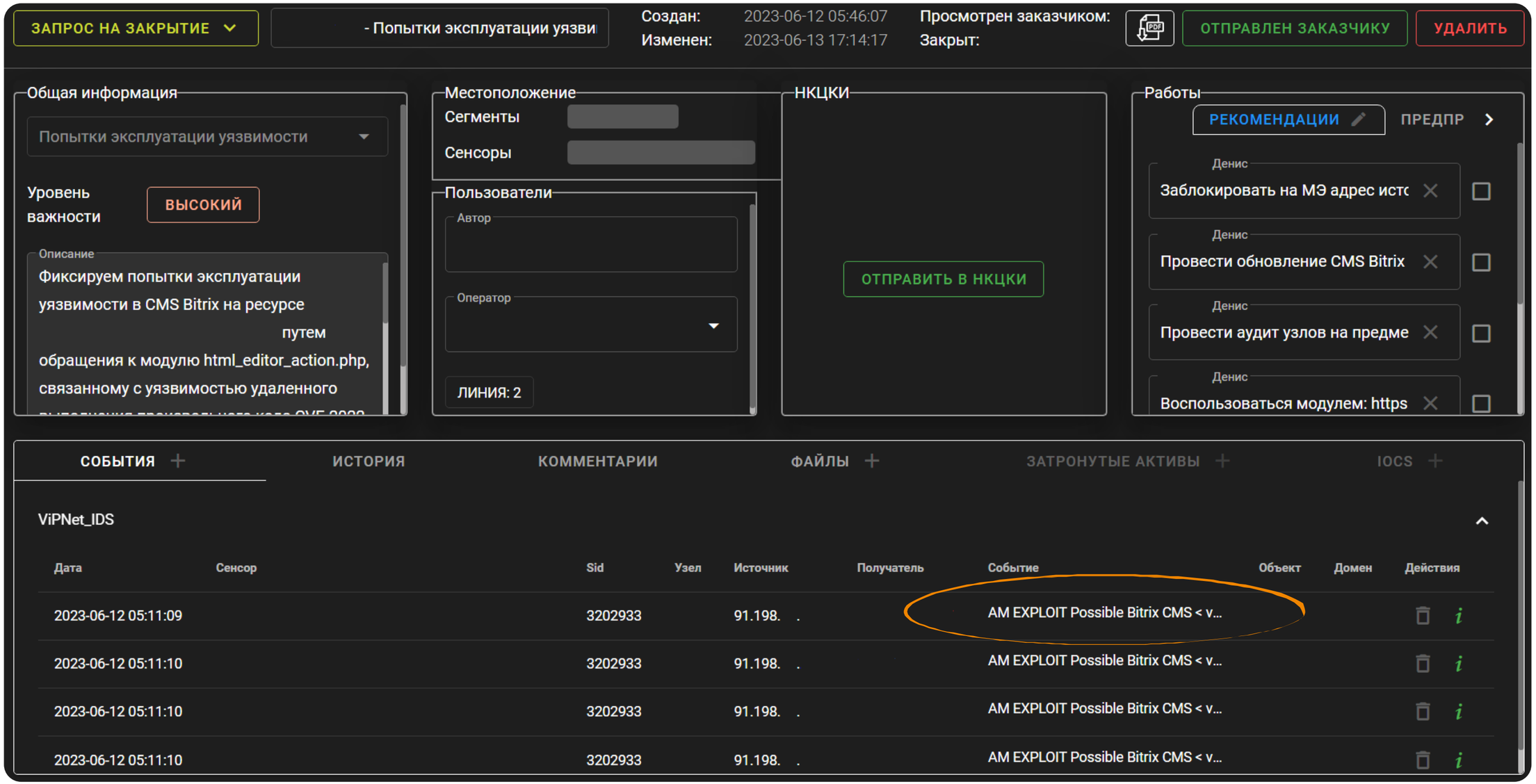
- sid 3204510 "AM EXPLOIT Google Chrome prior to v100.0.4896.88 RCE via devtools.inspectedWindow.eval (CVE-2022-1309)"
- sid 3204621 "AM EXPLOIT Possible Google Chrome prior to v104 UAF via LinkToTextMenuObserver (CVE-2022-2998)"
- sid 3203744 "AM EXPLOIT Possible Google Chrome prior to v103.0.5060.134 UAF via Service Worker API (CVE-2022-2480)"
- sid 3203379 "AM EXPLOIT Possible Google Chrome prior to v102.0.5005.61 Heap Buffer Overflow via uiDevTools (CVE-2022-1876)"
- sid 3204515 "AM EXPLOIT Google Chrome prior to v101.0.4951.41 UAF via BeginTransformFeedback (CVE-2022-1479)"
- sid 3204511 "AM EXPLOIT Google Chrome prior to v100.0.4896.88 RCE via RegExp.replace (CVE-2022-1310)"

Как использовать ЭД

для выявления подозрений на компьютерные инциденты или атаки



Пример использования:



Что может предложить АО «ПМ»

Snort / Suricata / yara / ossec

> 50 000 правил/сигнатур

URL-фильтрация

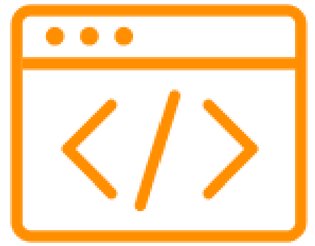
43 млн. доменов

IP, Domain, URL, Hash

STIX2.1, > 3,5 млн. IoC

Способы доставки ЭД

API



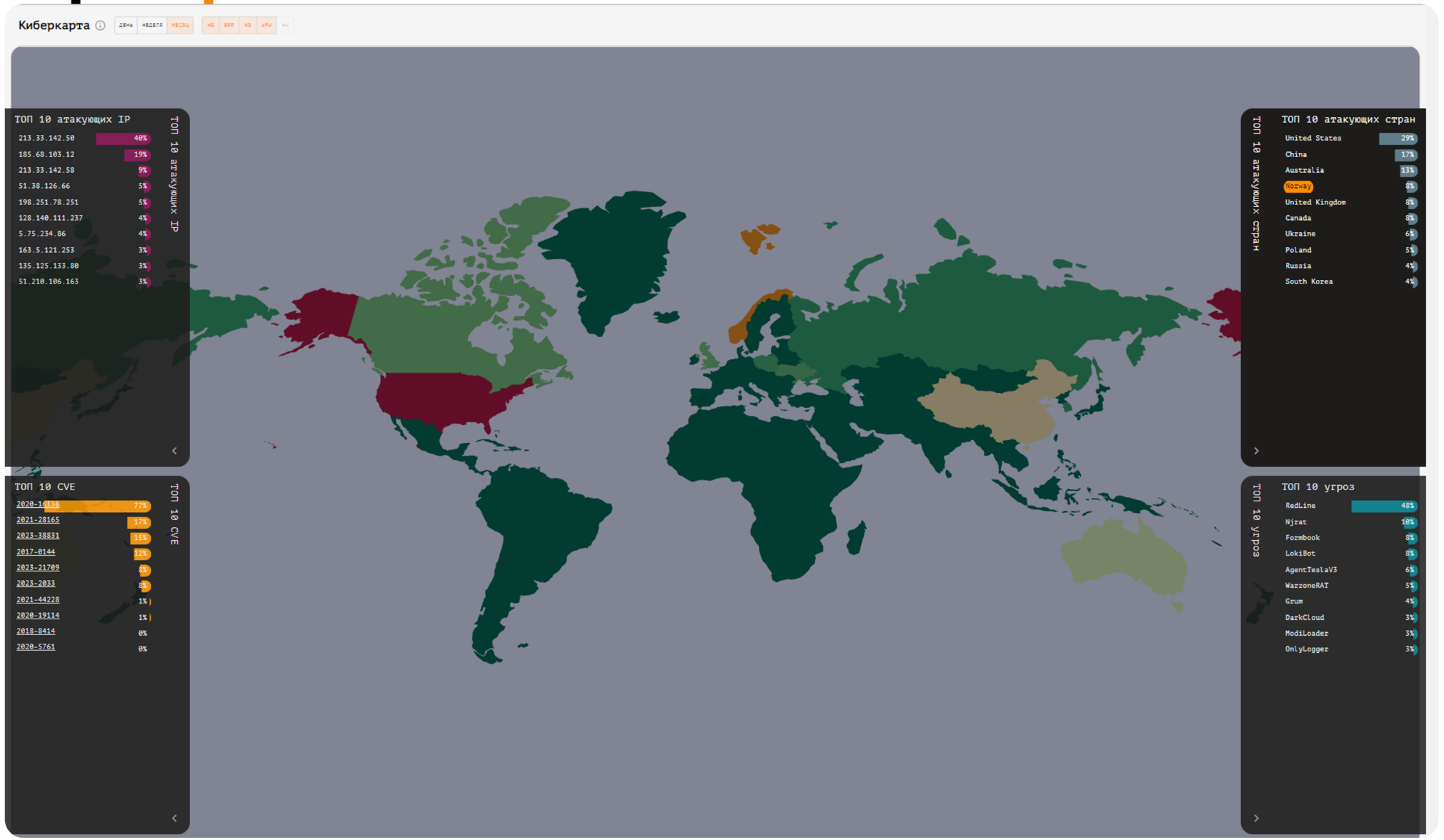
«Файлами»

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

AM Threat Intelligence Portal

Анонс нового продукта

Киберкарта


Киберкарта
ДЕНЬ
НЕДЕЛЯ
МЕСЯЦ
ТОП 10 атакующих IP
213.33.142.50 40%
185.68.103.12 19%
213.33.142.58 9%
51.38.126.66 5%
198.251.78.251 5%
128.140.111.237 4%
5.75.234.86 4%
163.5.121.253 3%
135.125.133.80 3%
51.210.106.163 3%
ТОП 10 атакующих стран
United States 29%
China 17%
Australia 13%
Norway 8%
United Kingdom 8%
Canada 8%
Ukraine 6%
Poland 5%
Russia 4%
South Korea 4%
ТОП 10 CVE
2020-14138 77%
2021-28165 17%
2023-38831 15%
2017-0144 12%
2023-21709 8%
2023-2033 8%
2021-44228 1%
2020-19114 1%
2018-8414 0%
2020-5761 0%
ТОП 10 угроз
RedLine 48%
Njrat 10%
Formbook 8%
LokiBot 8%
AgentTeslaV3 6%
WarzoneRAT 5%
Grum 4%
DarkCloud 3%
ModiLoader 3%
OnlyLogger 3%

Поиск по domain

pravokld.ru

ПОИСК

Обнаруженные угрозы

5/67

AM SCORE 0.8

Результаты для: pravokld.ru

Домен верхнего уровня: RU
Местонахождение: -

Метки образца: -
Чёрные списки: MyWOT BitDefender Fortinet

Категории: Malicious (alphaMountain.ai)

Правила/Сигнатуры 1

AM DNS Query for pravokld.ru associated with VBA/TrojanDownloader.Agent.LHL

Краткое описание

Правило реагирует на запрос к домену pravokld.ru, связанному с VBA/TrojanDownloader.Agent.LHL

Полное описание

Правило реагирует на запрос к домену pravokld.ru, связанному с VBA/TrojanDownloader.Agent.LHL

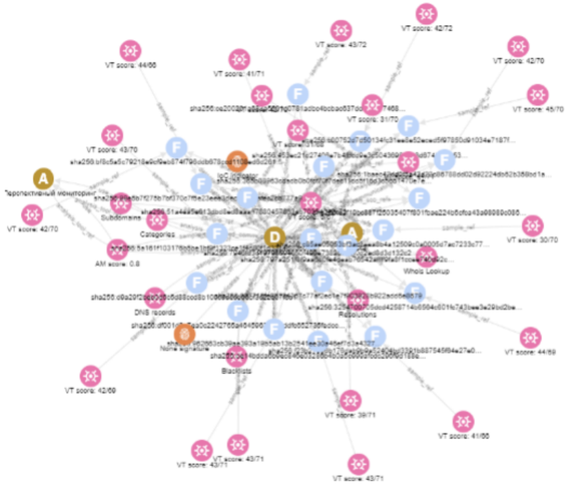
Критичность: Низкая
Типы атаки:
Платформы: -

Исходный текст

```
alert udp $HOME_NET any -> any 53 (msg:"AM DNS Query for pravokld.ru associated with
VBA/TrojanDownloader.Agent.LHL"; content:"|01 0000 01 000000000000|"; depth:10; offset:2;
content:"|08|pravokld|02|ru|00|"; fast_pattern; nocase; distance:0;
reference:url,virustotal.com/en/url/16ad17705391b43ad683660e5ff3450dbe9fa6878d5ce65f5f138beb3af2ad84/an
alysis; classtype:bad-unknown; sid:3040330; rev:3; metadata: affected_asset src, attack_target
Client_Endpoint, tias_category Malware;)
```

SNORT SURICATA

ЭКСПОРТ



Обзор

Whois: domain: PRAVOKLD.RU nserver: ns1.expired.reg.ru. nserver: ns2.expired.reg.ru. state: REGISTERED, DELEGATED, VERIFIED registrar: REGRU-RU created: 2017-02-17T14:13:48Z paid-till: 2019-02-17T14:13:48Z …
Связные IP-адреса: 185.165.123.36
Поддомены: www.pravokld.ru

Ресурсные записи DNS

Тип	Значение	ttl
A	192.12.94.30	509

Связи

Связанные URL-адреса

Дата	Ссылка	Detections
1 апр., 2019 03:42	http://pravokld.ru/g4iglrpspz	6 / 66
1 апр., 2019 03:42	http://pravokld.ru/Q4IOlRpsPz	7 / 66
1 февр., 2019 06:00	http://pravokld.ru/	5 / 67
13 нояб., 2018 02:17	http://pravokld.ru/Q4IOlRpsPz/	5 / 70
9 нояб., 2018 07:39	http://pravokld.ru/US/Documents/2018-11/	2 / 67
10 окт., 2018 01:30	http://pravokld.ru/CoastCapitalSavings.zip	1 / 67

Связанные хеш

Поиск по IP

149.248.34.200

поиск

Обнаруженные угрозы

1/71

AM SCORE 0.77

Результаты для: 149.248.34.200

Сеть: 149.248.0.0/18
ASN: 20473
Местонахождение: США, Сиэтл

Категории: -

Метки образца: win.systembc
Чёрные списки: threatfox

Правила/Сигнатуры 0

Сигнатуры не найдены

Обзор

Whois: NetRange: 149.248.0.0 - 149.248.63.255 CIDR: 149.248.0.0/18 NetName: CHOOP-1 NetHandle: NET-149-248-0-0-1 Parent: NET149 (NET-149-0-0-0-0) NetType: Direct Allocation OriginAS: AS20473 Organization: Cho…
Доменное имя: receitairpf2019.online
Выходной Tor-узел: Нет
Связанные домены: receitairpf2019.online

Связи

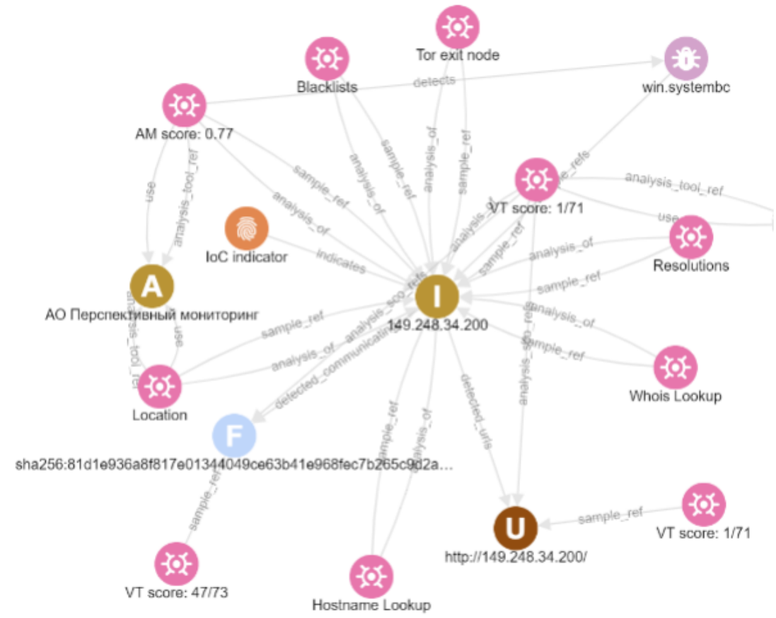
Связанные URL-адреса

Дата	Ссылка	Detections
12 мар., 2020 07:00	http://149.248.34.200/	1 / 71

Связанные хеш

Дата	Хеш	Detections
13 мар., 2020 04:46	81d1e936a8f817e01344049ce63b41e968fec7b265c9d2ab6678412904f15178	47 / 73

ЭКСПОРТ



Поиск по hash

81d1e936a8f817e01344049ce63b41e968fec7b265c9d2ab6678412904f15178

ПОИСК

Обнаруженные угрозы

47 /72

AM SCORE 0.65

Результаты для: 81d1e936a8f817e01344049ce63b41e968fec7b265c9d2ab6678412904f15178

Размер: 219.1 КБ
Дата первого появления: 27 мар., 2020 08:27
Дата последнего обновления: 15 мая, 2023 01:30
Тип файла: PE32 executable
TTP: TA0002, TA0007, TA0011, TA0043

Метки образца: Trojan-Proxy.Win32.Sybici.lg//Trojan.MulDrop11.47334
Чёрные списки: -

Категории: peexe overlay revoked-cert runtime-modules signed spreader direct-cpu-clock-access

Правила/Сигнатуры 0

Сигнатуры не найдены

Обзор

MD5: dceece60dcee5fd4d47755d6b3a85a75
SHA-1: 6969cc2f1939fd4373a83a2e607318e2cf7d78aa
SHA-256: 81d1e936a8f817e01344049ce63b41e968fec7b265c9d2ab6678412904f15178
SSDEEP: 3072:/kHyNZCT7RbVv513b2cLrEJeGUDL61UNmUCFh9W8Nf3IAK9EjCcak+OWgY5:VCTh/V3Deew893I/+UOXC
TLSH: T122244812760D44Ab7C63B02F1D8AD66B71E85EC804F2889CF4769DE5F66302C19C3316A
Размер: 219.1 КБ
Magic: PE32 executable

TrID: Win32 Executable MS Visual C++ (generic)(37.8%), Microsoft Visual C++ compiled executable (generic)(20%), Win64 Executable (generic)(12.7%), Win32 Dynamic Link Library (generic)(7.9%), Win16 NE executabl…

Связи

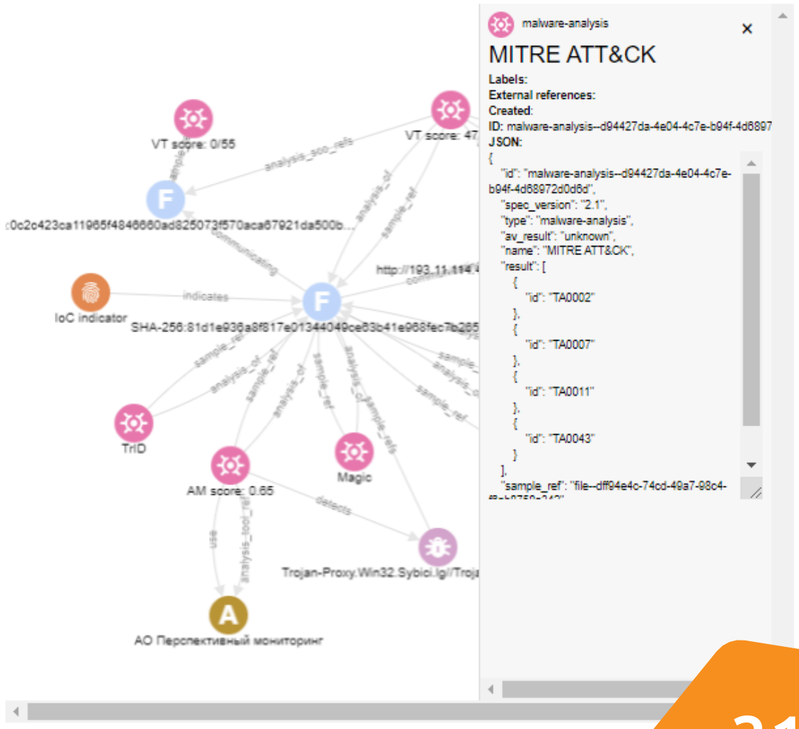
Связанные URL-адреса

Дата	Ссылка	Detections
Invalid Date	http://193.11.114.46:9032/tor/server/fp/cb6fc3a06fea1aab1d9b3a8afb2614887e0a3f3b	3 / 90

Связанные хеш

Дата	Хеш	Detections
Invalid Date	0c2c423ca11965f4846660ad825073f570aca67921da500b3d49f3cb39f68145	0 / 55

ЭКСПОРТ



Поиск по CVE

2023-38831

ПОИСК

Правила/Сигнатуры

sid	Время изменения	Название	Группы	TTP
3243782	12.09.23 03:15	AM CURRENT_EVENTS HTTP request to malicious IP endpoint in header 45.74.19.105 (WinRAR CVE-2023-38831 Usage)	emerging-current_events	TA0011
3243781	12.09.23 03:15	AM CURRENT_EVENTS HTTP request to malicious IP endpoint in header 153.92.126.196 (WinRAR CVE-2023-38831 Usage)	emerging-current_events	TA0011

Краткое описание

Правило реагирует на запрос к IP-адресу 153.92.126.196, связанному с WinRAR CVE-2023-38831 Usage

Полное описание

Правило реагирует на запрос к IP-адресу 153.92.126.196, связанному с WinRAR CVE-2023-38831 Usage

Критичность: Низкая
Типы атаки: Вредоносный ресурс
Платформы: -

Исходный текст

```
alert tcp $HOME_NET any -> any $HTTP_PORTS (msg:"AM CURRENT_EVENTS HTTP request to malicious IP endpoint
in header 153.92.126.196 (WinRAR CVE-2023-38831 Usage)"; threshold:type limit, track by_src, count 1,
seconds 120; content:"|0d0a|Host: 153.92.126.196|0d0a|";
reference:url,virustotal.com/en/url/d9b82810aa10d3077608cda7d3d262ef400a088b5d2405347816531206b9ff02/analy
sis; reference:url,group-ib.com/blog/cve-2023-38831-winrar-zero-day; classtype:trojan-activity;
sid:3243781; rev:1; metadata: affected_asset src, attack_target Client_Endpoint, tag TA0011,
tias_category Malware;)
```

SNORT SURICATA

3243780	12.09.23 03:15	AM DNS Query for trssp05923.com (WinRAR CVE-2023-38831 Usage)	emerging-dns	TA0011
3243779	12.09.23 03:15	AM DNS Query for tganngs9.com (WinRAR CVE-2023-38831 Usage)	emerging-dns	TA0011

Краткое описание

Правило реагирует на запрос к домену tganngs9.com, связанному с WinRAR CVE-2023-38831 Usage

Полное описание

Правило реагирует на запрос к домену tganngs9.com, связанному с WinRAR CVE-2023-38831 Usage

Критичность: Низкая
Типы атаки: Вредоносный ресурс
Платформы: -

Исходный текст

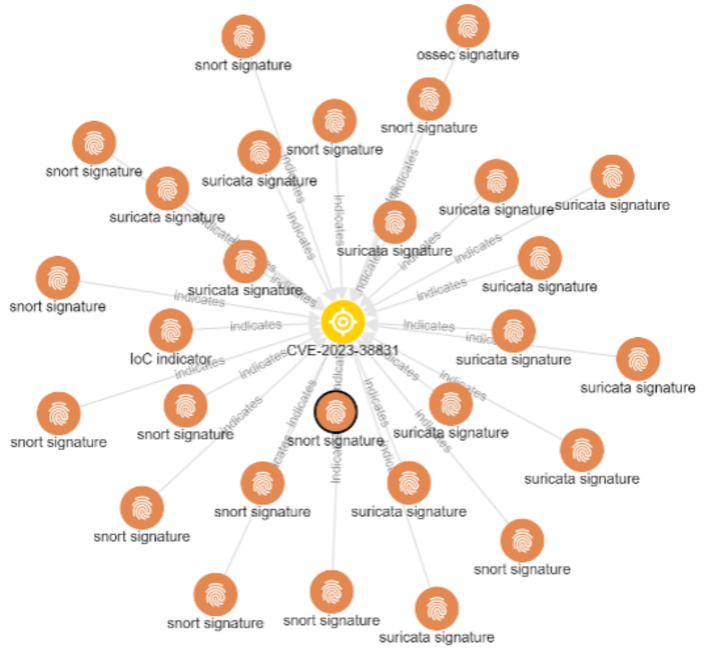
```
alert udp $HOME_NET any -> any 53 (msg:"AM DNS Query for tganngs9.com (WinRAR CVE-2023-38831 Usage)";
content:"|08|tganngs9|03|com|00|"; fast_pattern; nocase; distance:0;
reference:url,virustotal.com/en/url/380018a1f41d3238bac91db35f0eb89ef11c8a3d1eb59ce6515c3c2909694937/analy
sis; reference:url,group-ib.com/blog/cve-2023-38831-winrar-zero-day; classtype:trojan-activity;
sid:3243779; rev:1; metadata: affected_asset src, attack_target Client_Endpoint, tag TA0011,
tias_category Malware;)
```

SNORT SURICATA

3243778	12.09.23 03:15	AM DNS Query for mmnedgeggrrva.com (WinRAR CVE-2023-38831 Usage)	emerging-dns	TA0011

Записей на странице: 5 6-10 из 14

ЭКСПОРТ



Поиск по URL

http://fmc.org.in/wp-content/uploads/.libs/.password/index.inc.gif

ПОИСК

Обнаруженные угрозы

4/68

AM SCORE 0.8

Результаты для: http://fmc.org.in/wp-content/uploads/.libs/.password/index.inc.gif

Домен: fmc.org.in
Местонахождение: -

Метки образца: -
Чёрные списки: -

Категории: suspicious content | media sharing | blogs

Правила/Сигнатуры 0

Сигнатуры не найдены

Обзор

Whois: Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation…
Связанные домены: fmc.org.in

Связи

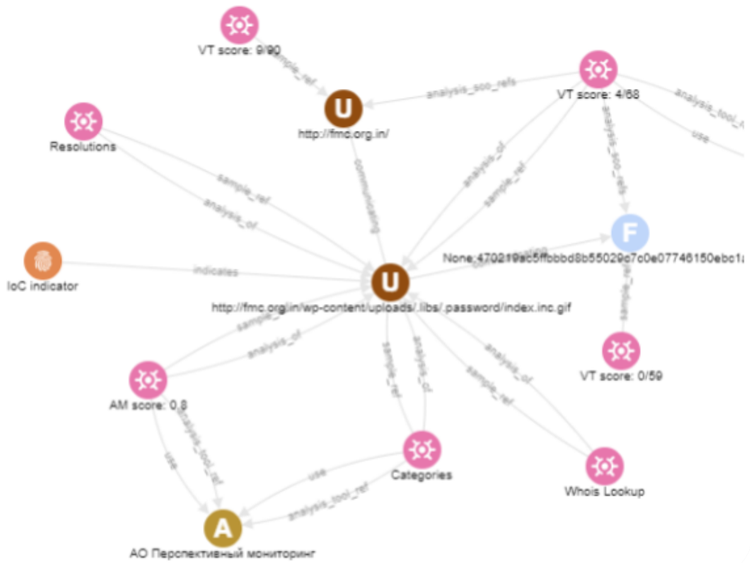
Связанные URL-адреса

Дата	Ссылка	Detections
Invalid Date	http://fmc.org.in/	9 / 90

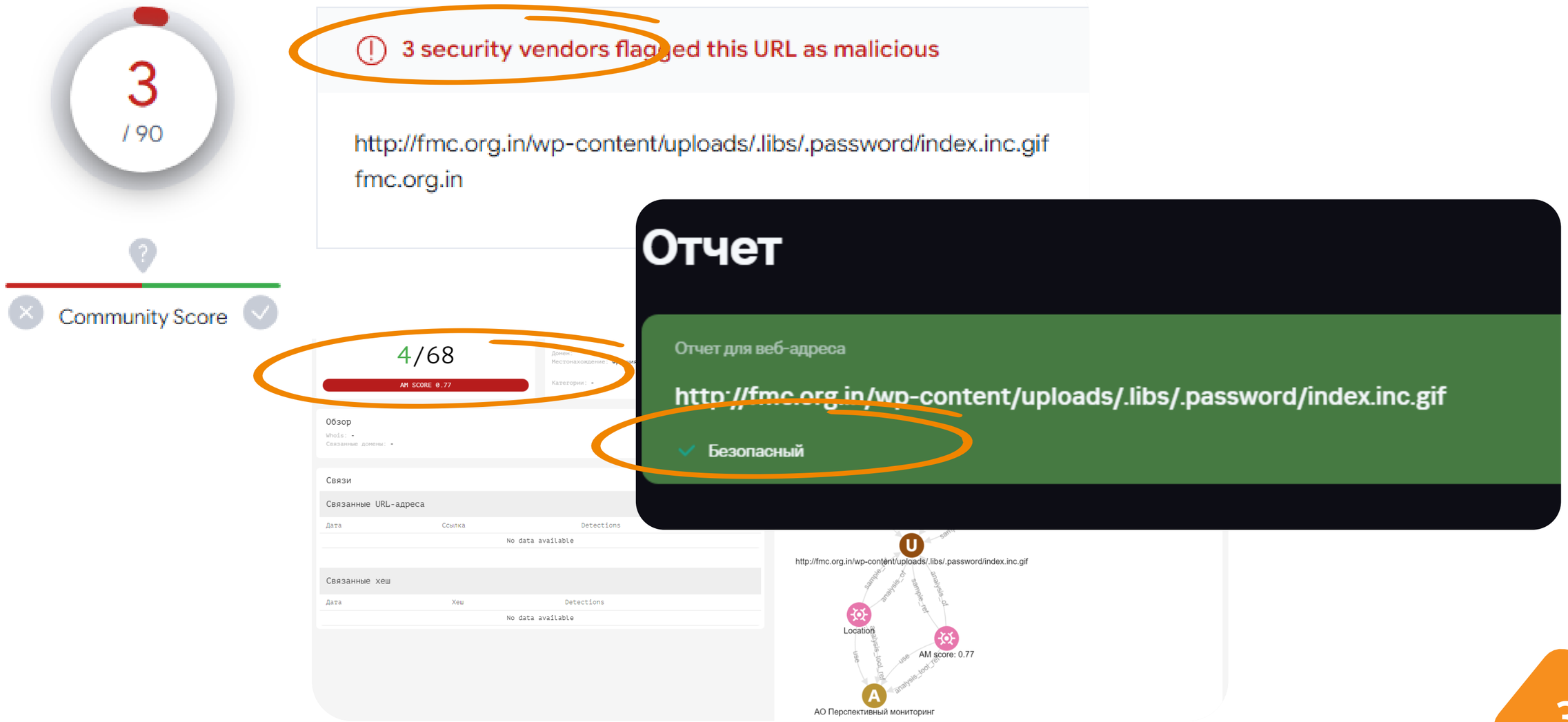
Связанные хеш

Дата	Хеш ↓	Detections
Invalid Date	470219ac5ffbbbd8b55029c7c0e0774615 0ebc1a4fb3f4165cd0328e78df415b	0 / 59

ЭКСПОРТ



В чём profit?


3
/ 90
Community Score
3 security vendors flagged this URL as malicious
http://fmc.org.in/wp-content/uploads/.libs/.password/index.inc.gif
fmc.org.in
4/68
AM SCORE 0.77
Обзор
Связи
Связанные URL-адреса
Дата
Ссылка
Detections
No data available
Связанные хеш
Хеш
Отчет
Отчет для веб-адреса
http://fmc.org.in/wp-content/uploads/.libs/.password/index.inc.gif
Безопасный
Location
AM score: 0.77
АО Перспективный мониторинг

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Артём Савчук

Заместитель технического директора,

«Перспективный мониторинг»

Artem.Savchuk@amonitoring.ru

t.me/pm_public

amonitoring.ru