ANGARA SOC

Векторы атак
Интересные особенности кейсов
Ход расследований (аналитика и индикаторы)
Рекомендации
Разница подходов злоумышленников к частным и государственным целям

ANGARA SOC

Начальник отдела
реагирования
и цифровой
криминалистики
Никита Леокумович

@LeokumovichN

n.leokumovich@angarasecurity.ru

+7 (914) 441-77-76

ANGARA SOC

Правовая оговорка (disclaimer)

Вся представленная информация получена законным путем.

Все нижеизложенное приводится исключительно
в информационных и образовательных целях.

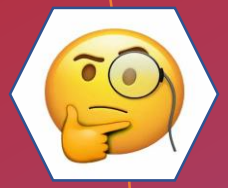
Повторение действий из презентации, возможно только с полного согласия СОБСТВЕННИКА информационной инфраструктуры, в которой выполняются действия.

Авторы запрещают применение действий из презентации
в незаконных целях.

Представленный материал не пропагандирует и не призывает
к совершению преступных деяний в отношении других лиц, компаний
и/или организаций, а также государства.

ANGARA SOC

Векторы атак



Интересные особенности кейсов

Ход расследований

Рекомендации

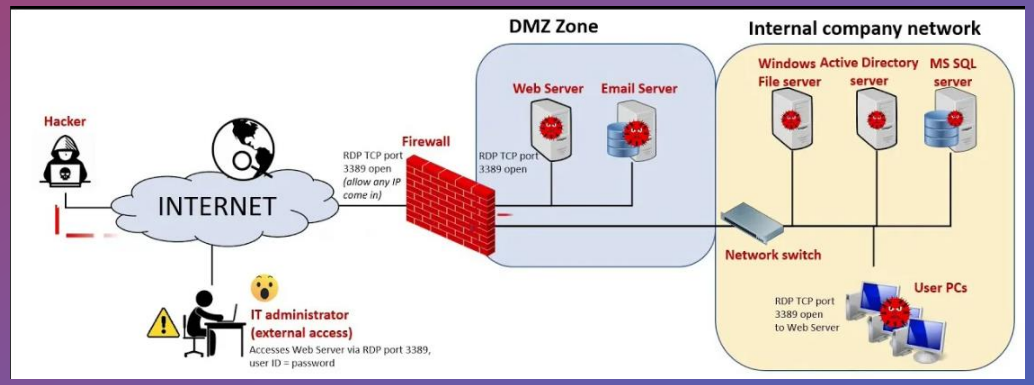
Разница подходов

Векторы атак

ANGARA SOC

Небольшие компании

Опубликованный в сеть
Интернет RDP порт



Использование уязвимостей
сервера электронной почты

“ProxyLogon”

CVE-2023-37580
CVE-2023-42115
CVE-2023-42116
CVE-2023-42117

Векторы атак

ANGARA SOC

Небольшие компании

«Утекшая» учетная запись Администратора

Векторы атак

ANGARA SOC

Крупные компании

Фишинг

Друзья, всем привет!

В преддверии новогодних праздников рады сообщить Вам о возможности приобритения самой настоящей красной икры с далёкой-далёкой Камчатки по цене в 100 рублей за 250 грамм! Если Вы хотите порадовать себя и своих близких, то сегодня же оставляйте свои заявки по адресу.

Спешите, так как предложение ~~не~~ограничено. :)

Для любителей элитного европейского алкоголя мы также подготовили предложение, которое сможет заинтересовать даже самого искушённого потребителя.

С уважением,

Менеджер по коммуникациям

Векторы атак

ANGARA SOC

Крупные компании

Проникновение в информационную инфраструктуру через подрядчиков

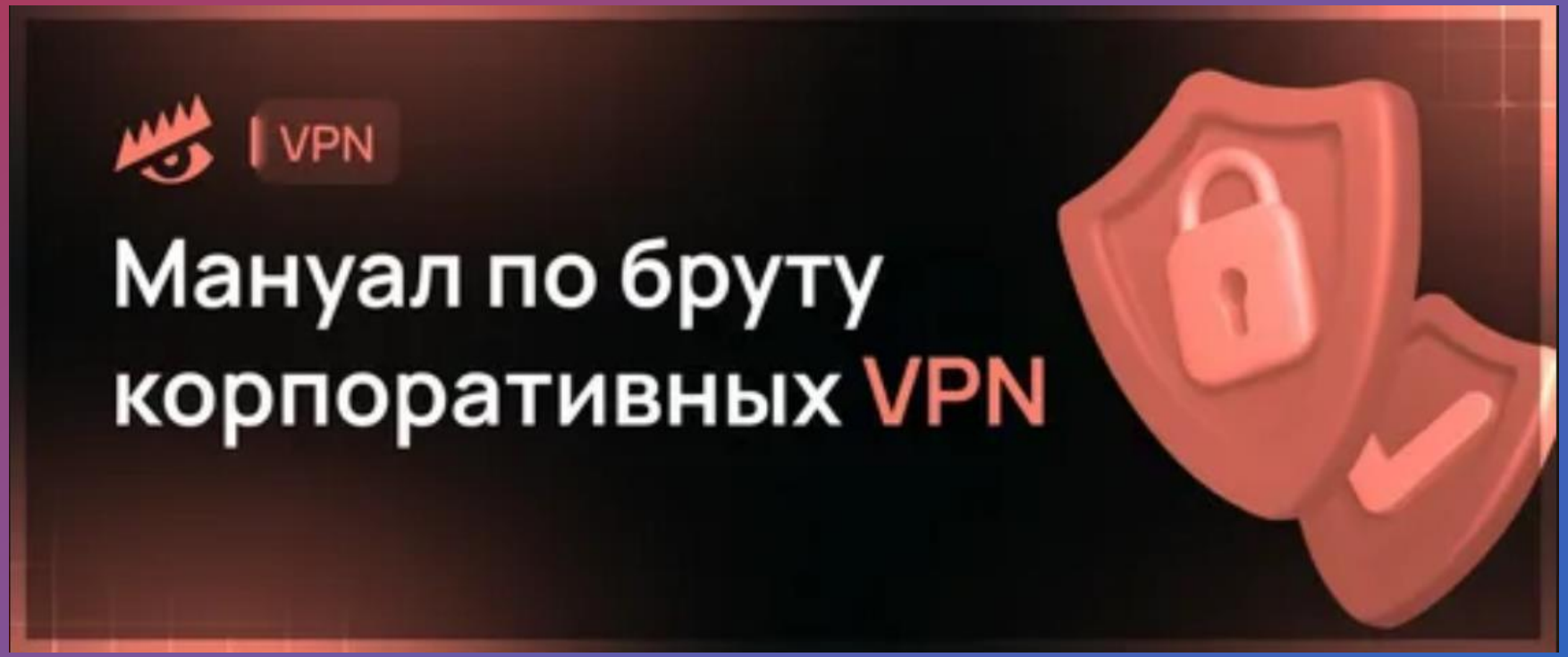
```
curl --location 'https:КРУПНАЯ КОМПАНИЯ' --header
'Authorization: Basic ЭТО ПОКАЗЫВАТЬ НЕЛЬЗЯ' --form
'username="ИМЯ ПОЛЬЗОВАТЕЛЯ"' --form
'password="ПАРОЛЬ В ОТКРЫТОМ ВИДЕ"' --form
'grant_type="password"'
```

Векторы атак

ANGARA SOC

Крупные компании

VPN

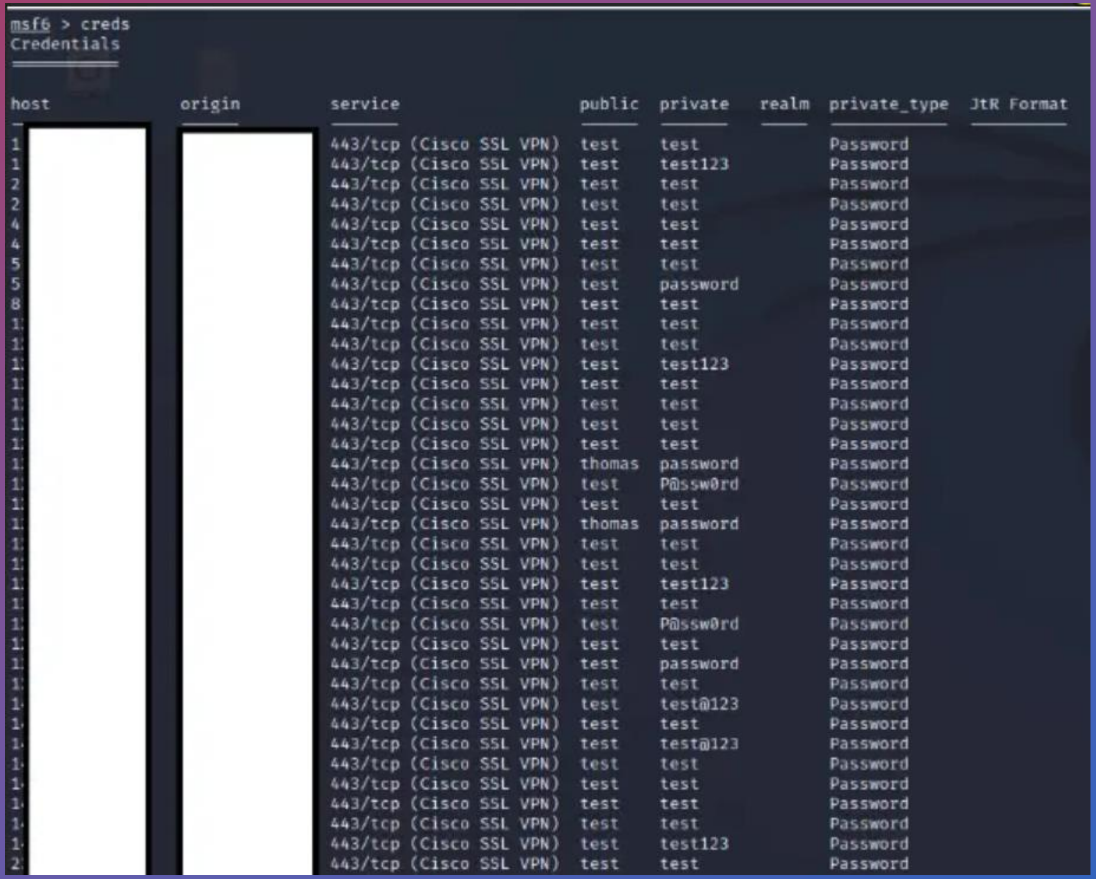


Векторы атак

ANGARA SOC

Крупные компании

VPN



msf6 > creds
Credentials
===========

host	origin	service	public	private	realm	private_type	JtR Format
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test123		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	password		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test123		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	thomas	password		Password	
		443/tcp (Cisco SSL VPN)	test	P@ssw0rd		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	thomas	password		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test123		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	P@ssw0rd		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	password		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test@123		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test@123		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	
		443/tcp (Cisco SSL VPN)	test	test123		Password	
		443/tcp (Cisco SSL VPN)	test	test		Password	

Векторы атак

ANGARA SOC

Государственные органы,
службы и крупные организации

Продвинутая постоянная угроза (Advanced Persistent Threat) - APT

Kasablanka
APT31

Mail-O

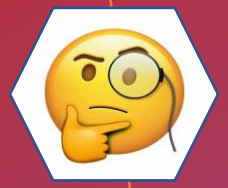
```
if ( !RegEnumKeyExA(hKey, 0, Name, &cchName, 0i64, 0i64, 0i64, 0i64) )
{
  while ( 1 )
  {
    v3 = (char *)&v15 + 95;
    do
      v4 = *++v3 == 0;
    while ( !v4 );
    strcpy(v3, "\\Software\\Mail.Ru\\Mail.Ru_Disko");
    if ( !RegOpenKeyExA(hKey, Name, 0, 0x20019u, &phkResult) )
      break;
    RegCloseKey(phkResult);
    ++v2;
    cchName = 256;
    if ( RegEnumKeyExA(hKey, v2, Name, &cchName, 0i64, 0i64, 0i64, 0i64) )
      goto LABEL_31;
  }
  cbData = 1000;
  Type = 1;
  RegQueryValueExA(phkResult, "InstallVer", 0i64, &Type, Data, &cbData);
  if ( cbData )
```

Webdav-O

```
00007FFC33EF3600  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00007FFC33EF3610  00 00 00 00 00 00 77 65  62 64 61 76 2E 79 61 6E  ......webdav.yan
00007FFC33EF3620  64 65 78 2E 72 75 00 00  00 00 00 00 00 00 00 00  dex.ru..........
00007FFC33EF3630  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00007FFC33EF3640  00 00 00 00 00 00 00 00  00 41 75 74 68 6F 72 69  .........Authori
00007FFC33EF3650  7A 61 74 69 6F 6E 3A 20  4F 41 75 74 68 20 25 73  zation:·OAuth·%s
00007FFC33EF3660  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00007FFC33EF3670  00 00 00 00 00 00 00 00  00 00 00 00 41 63 63 65  ............Acce
00007FFC33EF3680  70 74 3A 20 2A 2F 2A 0D  0A 41 75 74 68 6F 72 69  pt:·*/*..Authori
00007FFC33EF3690  7A 61 74 69 6F 6E 3A 20  4F 41 75 74 68 20 25 73  zation:·OAuth·%s
00007FFC33EF36A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 41  ...............A
00007FFC33EF36B0  63 63 65 70 74 3A 20 2A  2F 2A 0D 0A 44 65 70 74  ccept:·*/*..Dept
00007FFC33EF36C0  68 3A 20 31 0D 0A 41 75  74 68 6F 72 69 7A 61 74  h:·1..Authorizat
00007FFC33EF36D0  69 6F 6E 3A 20 4F 41 75  74 68 20 25 73 00 00 00  ion:·OAuth·%s...
00007FFC33EF36E0  00 00 3C 64 3A 68 72 65  66 3E 00 00 00 00 00 00  ..<d:href>......
00007FFC33EF36F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00007FFC33EF3700  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00007FFC33EF3710  00 00 00 00 00 3C 2F 64  3A 68 72 65 66 3E 00 00  .....</d:href>..
00007FFC33EF3720  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00007FFC33EF3730  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

ANGARA SOC

Векторы атак



Интересные особенности кейсов

Ход расследований

Рекомендации

Разница подходов

ANGARA SOC

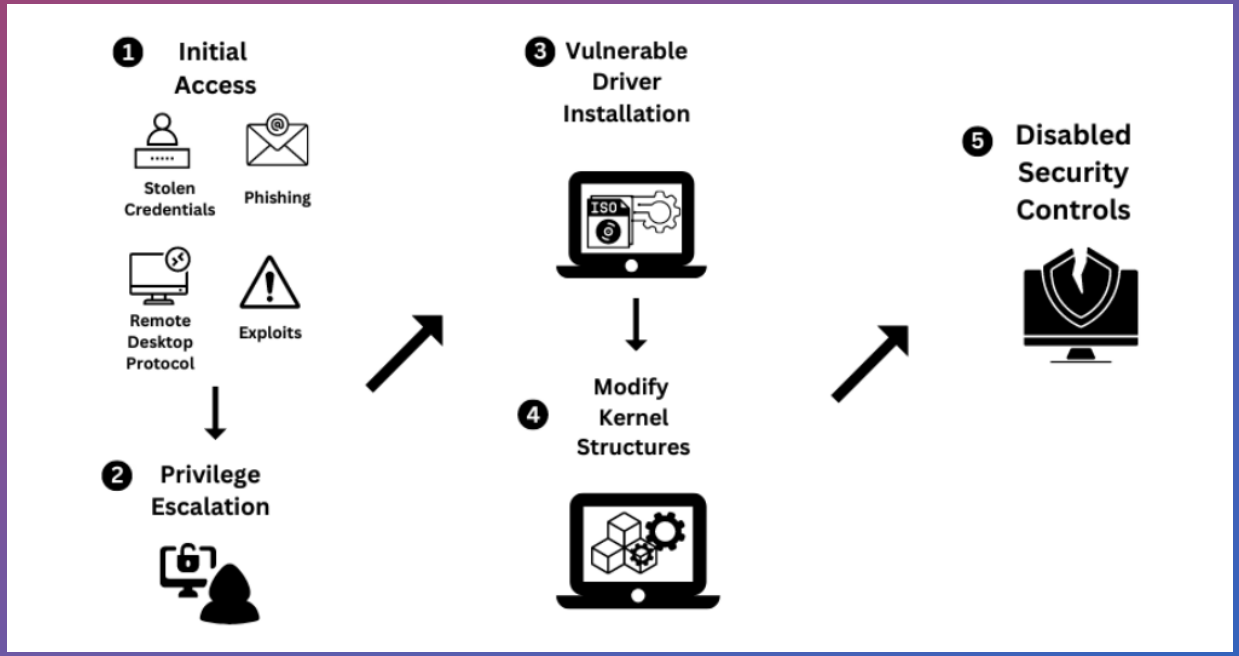
Интересные особенности кейсов

«Угон» Telegram

ANGARA SOC

Интересные особенности кейсов

Bring Your Own Vulnerable Driver



ANGARA SOC

Интересные особенности кейсов

Living off the land

PowerShell
Task Scheduler Configuration Tool (schtasks.exe)
Scheduled Service Command Line Interface (at.exe)
Microsoft HTML Application host (MSHTA.exe)
Registry Console Tool (reg.exe)
Windows Management Instrumentation Command-Line (wmic.exe)
Service Control Manager Configuration Tool (sc.exe)

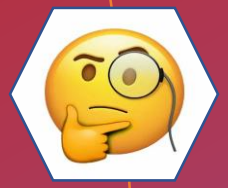
ANGARA SOC

Интересные особенности кейсов

Веди себя как пользователь
(User like)

ANGARA SOC

Векторы атак



Интересные особенности кейсов

Ход расследований

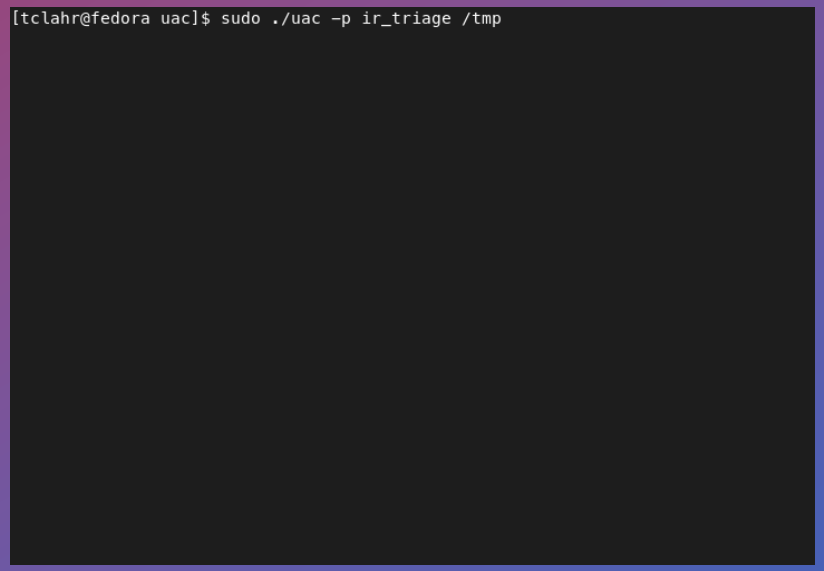
Рекомендации

Разница подходов

ANGARA SOC

Ход расследований

Сбор криминалистически значимых артефактов (Triage)



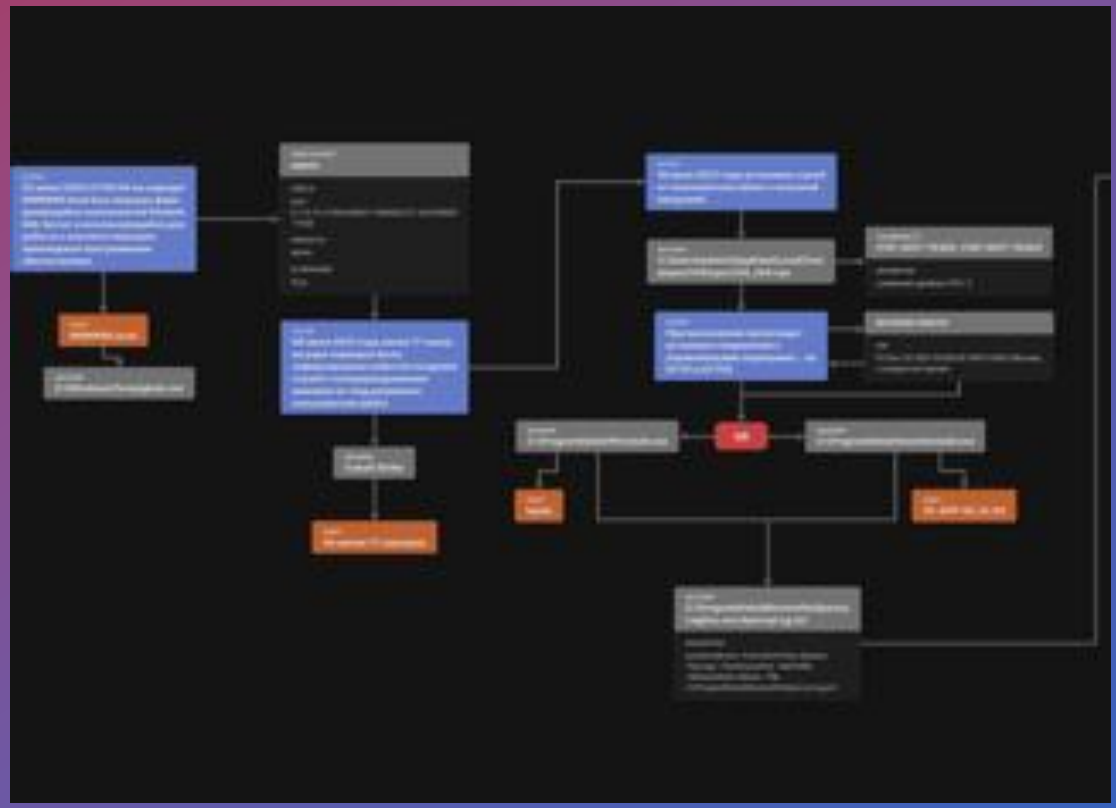
Топ утилит для создания Forensic Triage: их особенности и возможности **Камиль Камалетдинов**

https://habr.com/ru/companies/angarasecurity/articles/718500/

ANGARA SOC

Ход расследований

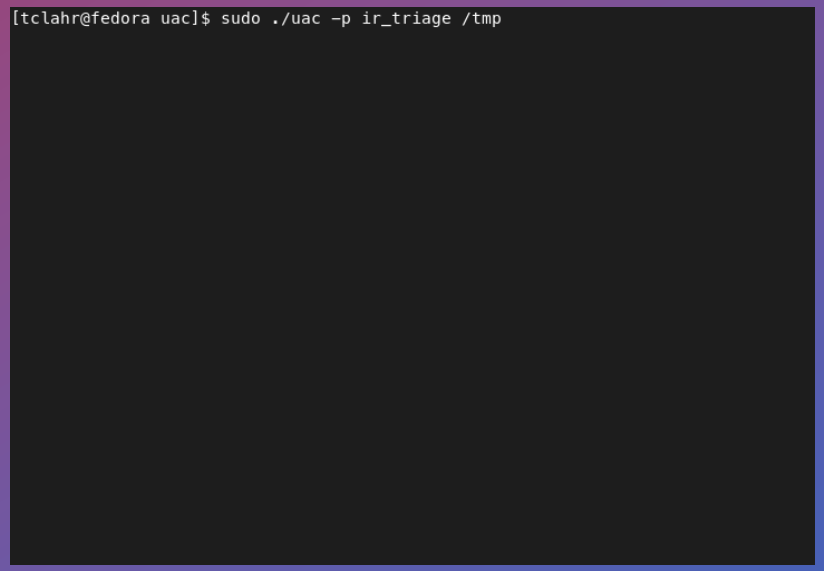
Раскручиваем цепочку



ANGARA SOC

Ход расследований

Сбор криминалистически значимых артефактов (Triage)



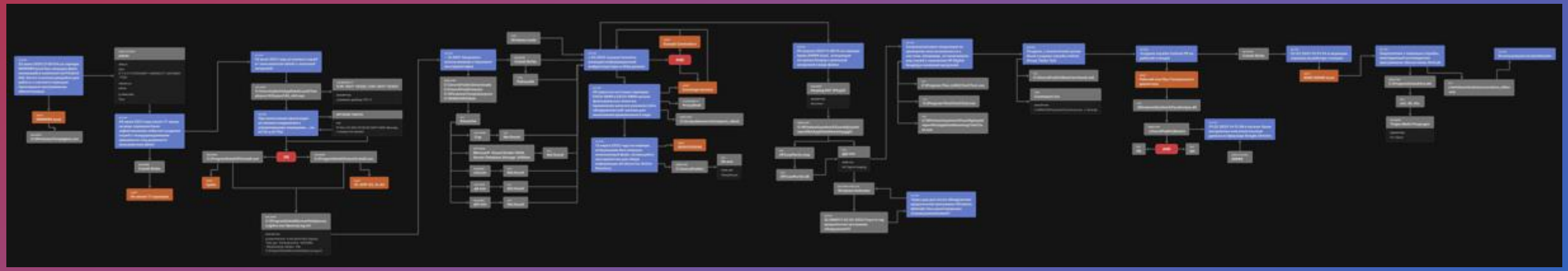
Топ утилит для создания Forensic Triage: их особенности и возможности **Камиль Камалетдинов**

https://habr.com/ru/companies/angarasecurity/articles/718500/

ANGARA SOC

Ход расследований

Раскручиваем цепочку



ANGARA SOC

Ход расследований

ANGARA
SOC

РЕЗУЛЬТАТЫ АНАЛИЗА ДАННЫХ

НОЯБРЬ 2023

ANGARA
SOC

ОТЧЕТ ОБ АУДИТЕ
ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

НОЯБРЬ 2023

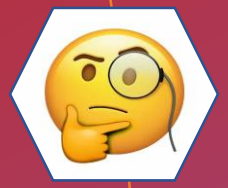
ANGARA
SOC

ОТЧЕТ
О РЕАГИРОВАНИИ НА ИНЦИДЕНТ

НОЯБРЬ 2023

ANGARA SOC

Векторы атак



Интересные особенности кейсов

Ход расследований

Рекомендации

Разница подходов

Рекомендации

ANGARA SOC

Управление активами

Рекомендации

ANGARA SOC

AD TIER

Рекомендации

ANGARA SOC

LAPS, LDAPS,
отключение LM & NTLMv1,
анонимного доступа к AD, и т.д.

Рекомендации

ANGARA SOC

Настройки аудита

Рекомендации

ANGARA SOC

2FA

Рекомендации

ANGARA SOC

Общие правила Ubuntu.com

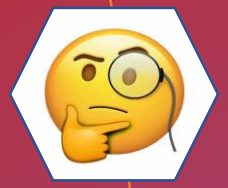
40 Linux Server Hardening Security Tips [2023 edition]

The 50 Best Linux Hardening Security Tips: A Comprehensive Checklist

Linux Server Hardening and Security Best Practices

ANGARA SOC

Векторы атак



Интересные особенности кейсов

Ход расследований

Рекомендации

Разница подходов

Разница подходов

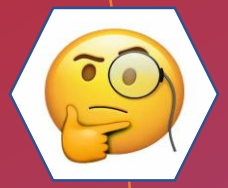
ANGARA SOC

Частные компании

Государственные учреждения

ANGARA SOC

Вывод



Относитесь к информационной безопасности своей информационной инфраструктуры как к своей личной безопасности. Используйте средства защиты информации и мониторьте события ИБ.

Эти меры позволят вам сохранить свою информационную инфраструктуру в безопасности, избежать финансовых и репутационных рисков.

ANGARA SOC

Спасибо за внимание!

Начальник отдела реагирования и цифровой криминалистики

Никита Леокумович

@LeokumovichN

n.leokumovich@angarasecurity.ru

+7 (914) 441-77-76