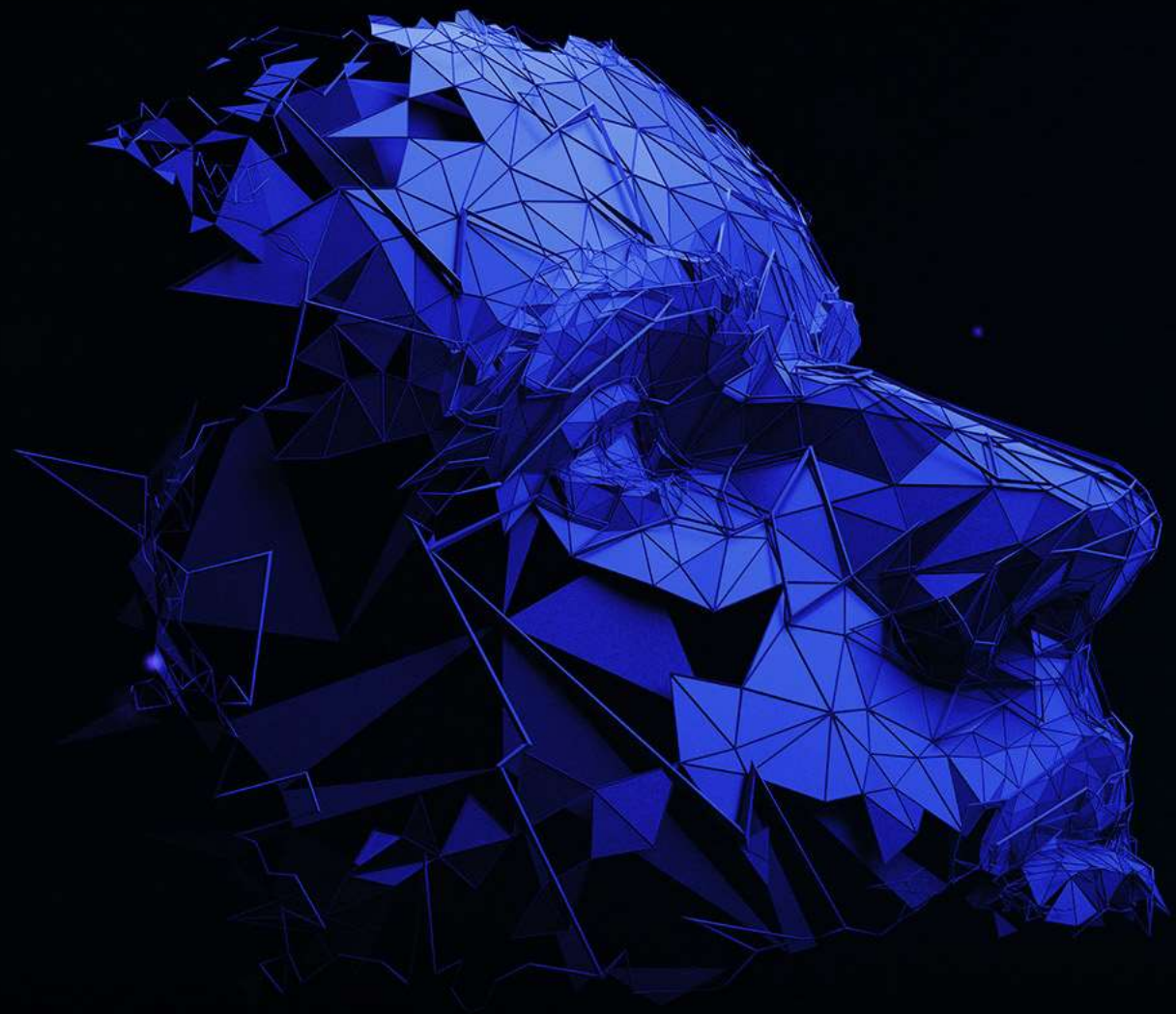
BI.ZONE

Нарушая правила

Как злоумышленники используют ВПО, распространяемое на теневых ресурсах, в атаках на российские организации

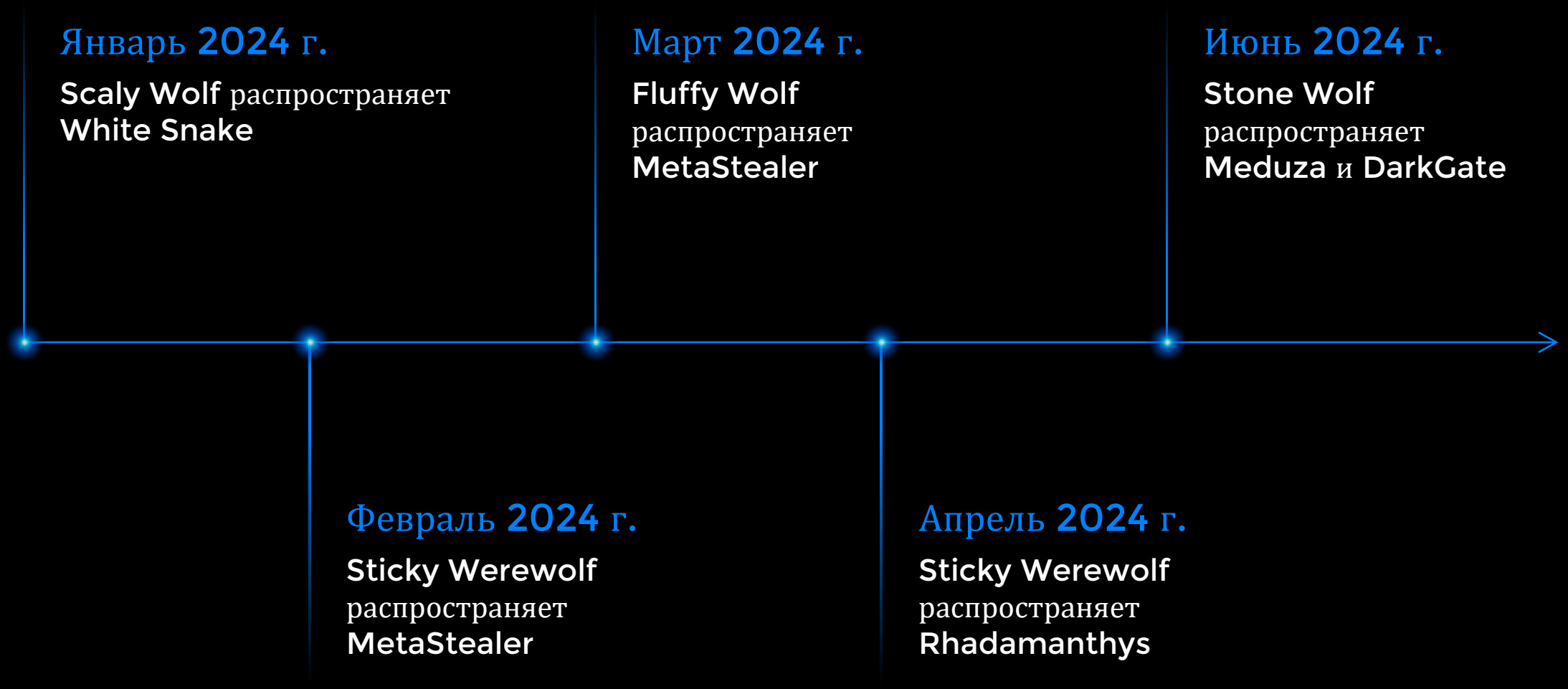


Олег Скулкин

Руководитель BI.ZONE Threat Intelligence

BI.ZONE

Если проблему можно решить деньгами, это не проблема — это расходы!

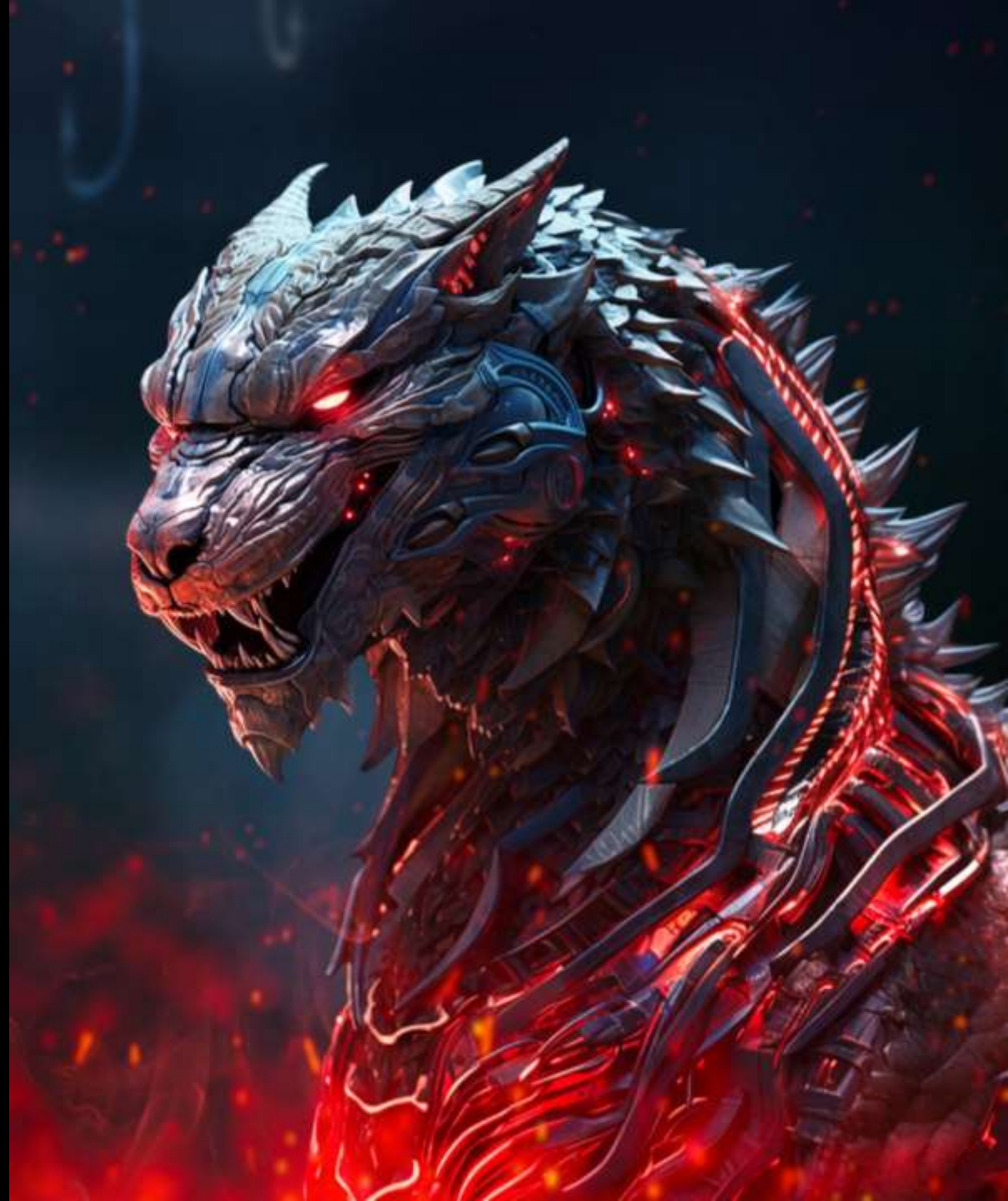

Январь 2024 г.
Scaly Wolf распространяет White Snake
Февраль 2024 г.
Sticky Werewolf распространяет MetaStealer
Март 2024 г.
Fluffy Wolf распространяет MetaStealer
Апрель 2024 г.
Sticky Werewolf распространяет Rhadamanthys
Июнь 2024 г.
Stone Wolf распространяет Meduza и DarkGate

BI.ZONE

Scaly Wolf

Кластер, активный с начала **2023** года.
Использует фишинговые электронные письма для получения первоначального доступа, рассылая их от имени различных ведомств.
Атакует организации разных отраслей на территории России и Белоруссии.

Имеет в арсенале как инструменты собственной разработки, так и коммерческие – например, стилер **White Snake**.
Преимущественно занимается кражей конфиденциальных данных



BI.ZONE

White Snake

Распространяется на теневых ресурсах с февраля 2023 года

Доступна как версия для Windows, так и версия для Linux

Позволяет атакующему не только получить аутентификационный материал, но и решать различные задачи постэксплуатации

Позиционируется как инструмент для проведения целевых атак

Месячная подписка стоит 200 $, бессрочная – 1950 $

BI.ZONE

Возможности обнаружения

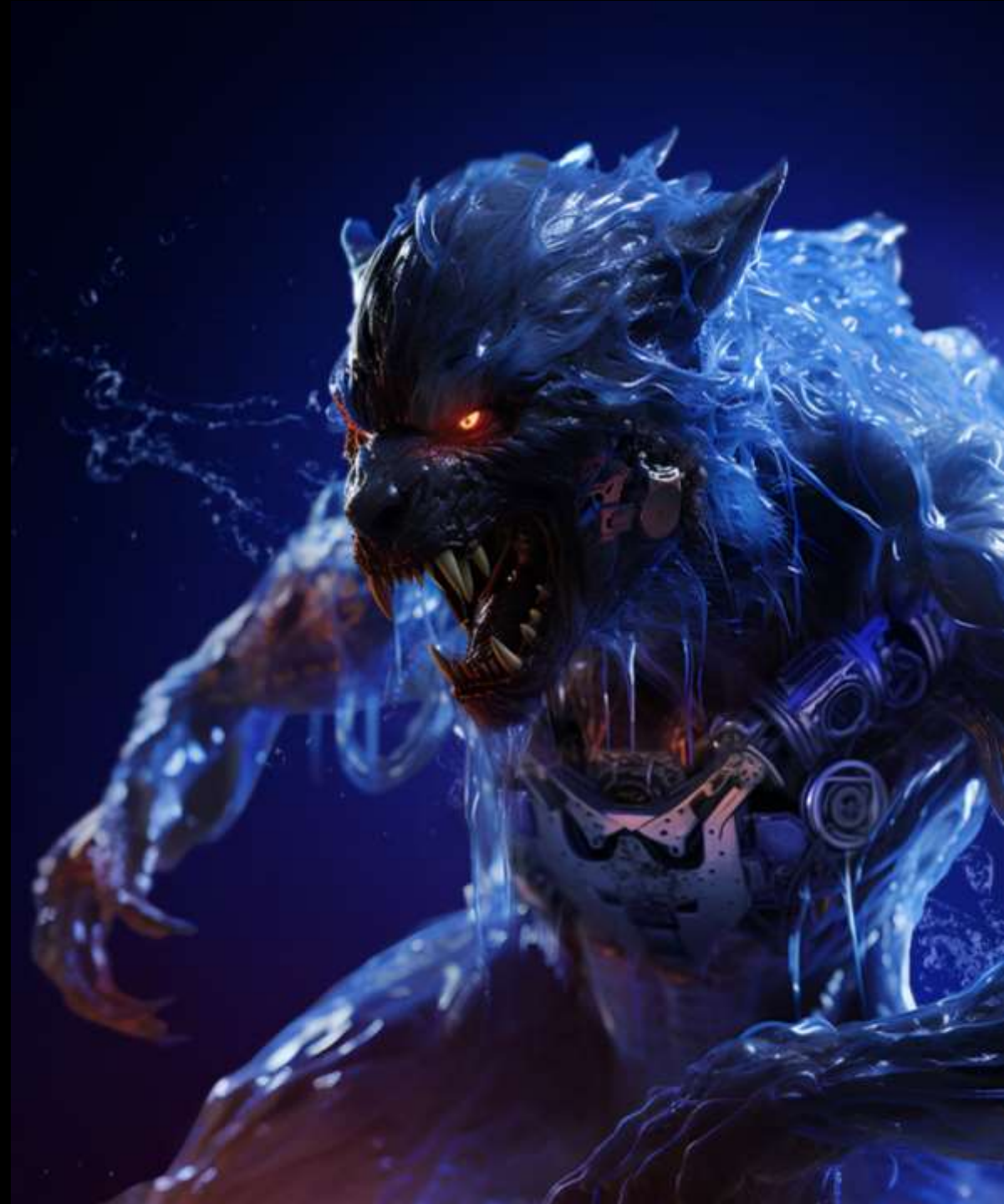
- Характерные параметры командной строки, использующиеся для создания заданий в планировщике **Windows**, например: chcp 65001 && ping 127.0.0.1 && schtasks
- Сбор информации о скомпрометированной системе с помощью **WMI**, например: SELECT * FROM Win32_LogicalDisk WHERE DriveType = 3 – Size
- Получение **IP**-адреса скомпрометированной системы с использованием ресурса http://ip-api[.]com/line?fields=query,country
- Взаимодействие с файлами, в которых хранятся пароли, нетипичными исполняемыми файлами
- Индикаторы компрометации, связанные со стилером **White Snake** и **Scaly Wolf**

BI.ZONE

Sticky Werewolf

Кластер, активный как минимум с апреля **2023** года. Атакует преимущественно Россию и Белоруссию с целью шпионажа. Получает первоначальный доступ к целям через фишинговые рассылки.

Имеет в арсенале широкий набор вредоносного программного обеспечения, например: **Ozone RAT**, **Darktrack RAT**, **Quasar RAT**, **MetaStealer**, **Glory Stealer**, а также **Rhadamanthys Stealer**



BI.ZONE

Rhadamanthys

Распространяется
на теневых ресурсах
с сентября 2022 года

Позволяет получить
учетные данные
из браузеров,
кошельков и т. п.

Также позволяет атакующим
выполнять команды
в PowerShell
и осуществлять сбор файлов
по заданным критериям

Позиционируется как
стилер «все в одном»

Стоимость месячной
подписки начинается всего
от 59 $

BI.ZONE

Возможности обнаружения

- Использование **findstr** и **tasklist** для поиска процессов, связанных с АВПО, например:
  `tasklist | findstr /I “wsra.exe opssvc.exe”`

- Взаимодействие с файлами, в которых хранятся пароли, нетипичными исполняемыми файлами, например: **dialer.exe**

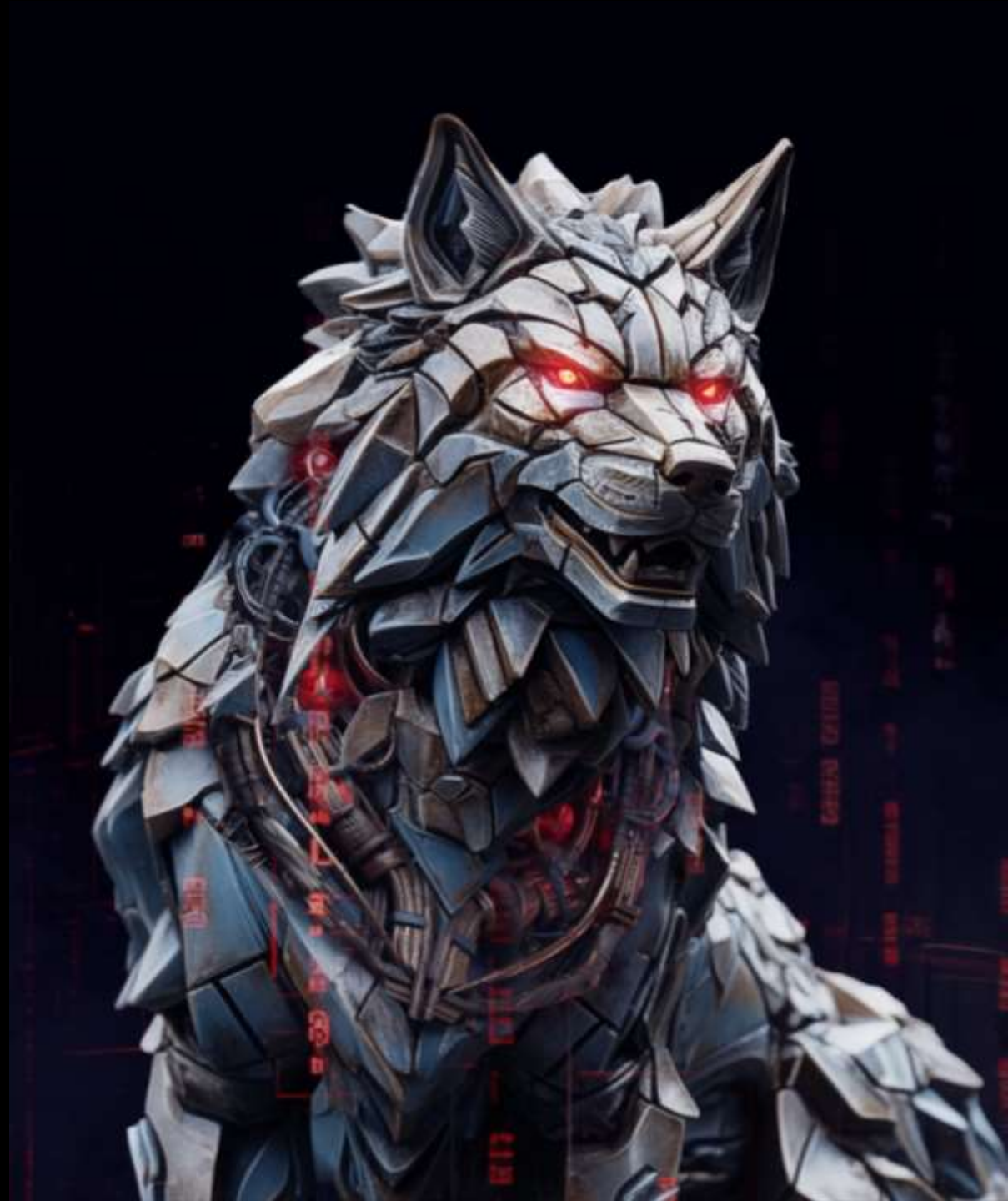
- Мьютекс формата `Global\MSCTF.Asm.{digits}`

- Индикаторы компрометации, связанные со стилером **Rhadamanthys** и **Sticky Werewolf**

Stone Wolf

Кластер, активный как минимум с мая **2024** года. Использует фишинговые письма для получения первоначального доступа.

В арсенал злоумышленников входит **Meduza**, а также **DarkGate** и **Remcos**



BI.ZONE

DarkGate

Распространяется на теневых ресурсах с июня 2023 года

Может выполнять функции загрузчика, стилера и RAT

ВПО поддерживает широкий набор команд, которые позволяют решать любые задачи в контексте постэксплуатации

Позиционируется как загрузчик, разрабатываемый с 2017 года

Стоимость месячной подписки – 15 000 $, годовой – 100 000 $

BI.ZONE

Возможности обнаружения

- Запуск сценариев с помощью интерпретатора AutoIt
  из временных папок и иных подозрительных расположений

- Сбор информации о системе с помощью **wmic** и ее сохранение
  в подпапки **ProgramData**, например:
  `wmic ComputerSystem get domain > C:\ProgramData\bcabbfb\cddfhbc`

- Поднятие привилегий с использованием **PsExec**:
  `cmd /c c:\temp\PsExec.exe -accepteula -j -d -s [путь к файлу]`

- Запуск архиватора WinRAR со следующими параметрами: `a -ep1 -r -y -v5m -m1`

- Индикаторы компрометации, связанные с **DarkGate** и **Stone Wolf**

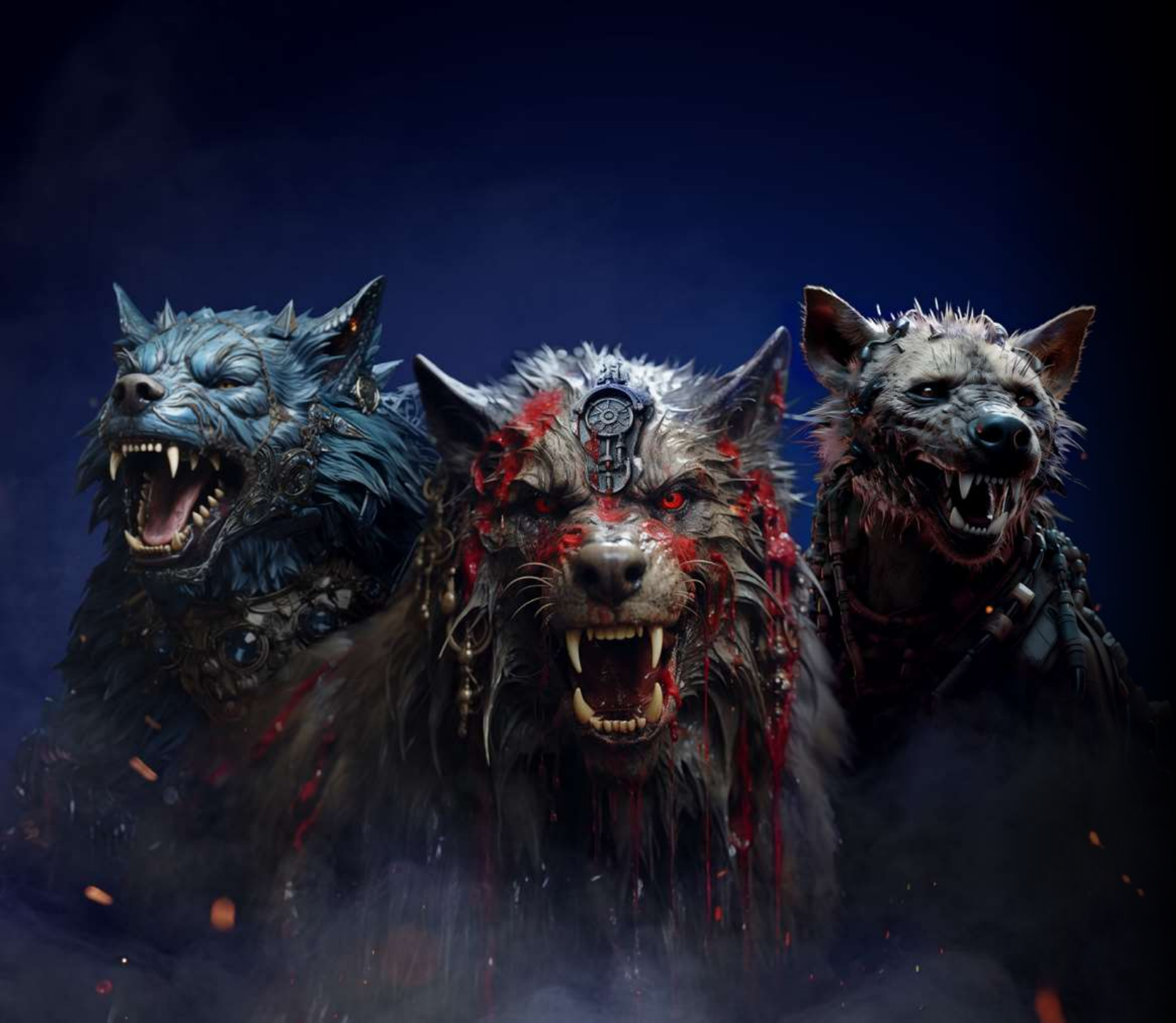
BI.ZONE

Ключевые выводы

Злоумышленникам совсем не обязательно заниматься разработкой инструментария: сегодня многое доступно в открытых источниках,
а также на теневых ресурсах.

Несмотря на то что исторически злоумышленник не использовали инструменты, распространяющиеся через русскоязычные теневые форумы, для реализации атак в регионе, сегодня это правило часто нарушается.

Своевременное получение информации о методах и инструментах злоумышленников позволяет обнаруживать попытки их применения на ранних этапах жизненного цикла атаки и избежать нанесения возможного ущерба



Спасибо за внимание!

Узнайте больше о локальном ландшафте угроз