

ATHENA

Система защиты от целенаправленных атак

Техническое описание

Описание проблемы

Целенаправленные атаки быстро совершенствуются, применяя технологии искусственного интеллекта и средства обхода современных инструментов защиты. Одним из распространенных способов их осуществления является вредоносное программное обеспечение.

Решение

Система защиты от целенаправленных атак AVSOFT ATHENA обеспечивает безопасность организаций уже более 15 лет, используя большое количество инструментов анализа в сочетании с технологиями искусственного интеллекта.

Решение способно принимать почтовый, сетевой и веб-трафик, а также данные от любых автоматизированных систем по протоколу ICAP и API интерфейсу.

Виды трафика

- Веб-трафик
- Почтовый трафик
- Сетевой трафик
- Рабочие места и сервера
- Файловые хранилища

Виды протоколов

- ICAP
- AD/LDAP
- SMTP
- FTP (S)
- Syslog
- SMB
- API
- NFS

Система AVSOFT ATHENA эффективно противодействует широкому спектру киберугроз

Сетевые черви	Эксплойты и скрипты
Троянские программы	Криптомайнеры
Руткиты	Ботнеты
Буткиты	Вайперы
Рекламное ПО	Стилеры
Шифровальщики	Фишинг

Инструменты анализа

Решение имеет самое большое количество инструментов анализа на рынке, которые подразделяются на статический, динамический фишинговый анализ

Статический анализ



Возможность бесшовной интеграции с внешними антивирусными движками



Детальный анализ структуры и содержимого файлов



Проверку во внешних аналитических ресурсах и репутационных базах



Анализ определенных типов файлов в соответствующих нейронных сетях



Распаковку архивов, включая многотомные и защищенные паролем

Динамический анализ

Динамическое направление проверки дополняет статическое направление. т.к. антивирусные базы данных не всегда содержат сигнатуры нового вируса. Оно включает в себя исследование поведения ПО в изолированных виртуальных и физических средах («песочницах»), имитирующих компьютер или мобильное устройство.

Внутри «песочниц» установлен контент и автоматическая имитация работы пользователя. Вердикт динамического анализа выносится на основании зафиксированных подозрительных или вредоносных действий исследуемого файла в имитационной среде – «песочнице».

Они могут быть кастомизированы под контент и состав ПО реального предприятия.

В динамическом анализе осуществляется также фиксация потребляемых ресурсов, что позволяет выявить ПО, расходующее ресурсы ОС для майнинга. После сбора событий о поведении ПО внутри «песочницы» происходит их анализ и определение вердикта.

Система ATHENA имеет широкую линейку поддерживаемых операционных систем в динамическом анализе

Windows

- Windows 7
- Windows 10
- Windows Server 2016
- Windows Server 2019

Android

- Android 10
- Android 11
- Android 12
- Android 13
- Android 15

Linux

- Astra SE 1.7.3 (5.4)
- Astra-OREL 2.12.45 (5.4)
- Astra-OREL 2.12.4 (4.16)
- Centos 8 (4.18)
- Debian-9.4.0 (4.16)
- OpenSUSE Leap 15.5 (5.14)
- RedOS Murom 7.2 (4.19)
- Ubuntu 20.04 (5.4)
- Ubuntu 22.04 (6.2)

Анализ ссылок

Система AVSOFT ATHENA осуществляет статический и динамический анализ веб-ссылок

Инструменты анализа ссылок

-  Динамика переходов по ссылке и коды ответов
-  Содержимое страницы (анализ кода страницы и js)
-  Анализ скриншотов веб-страниц
-  Анализ DNS, сертификата SSL, владельца и др.
-  Внешние сервисы (Alexa, Whois, PageRank и др)

Типы проверяемых ссылок

-  Веб-ссылки
-  Прямые и не прямые
-  На облака и файловые хранилища
-  IP адреса
-  С переходами, в том числе с отложенными (meta-refresh)

Система ATHENA способна принимать любые типы файлов на проверку

Архив	.7z, .arj, .bz2, .cab, .deb, .gz, .gzip, .iso, .jar, .one, .rar, .rpm, .tar, .xz, .zip, .lhz, .z, .deb, .r01, .lha, .ice, .tar.gz, .tgz
Документ	.chm, .cpp, .doc, .docm, .dot, .kml, .odp, .ods, .odt, .one, .pdf, .ppsx, .rtf, .svg, .txt, .xls, .dotm, .potm, .ppsm, .ppsx, .pptm, .pptx, .xlsb, .xlsm, .xlsx, .docx, .ppsm, .ppt, .xltm, .scr, dotx, potx, .xlam, .ppam, .txt, .appx, ott, odg, ots, xla, xlam, xlt, xltx, .pot, .ppa, .sldm, .sldx, .pub, .tgz, .odm, .log, .wps, .ace, .php, .mht, .asp, .pps, .xll, .slk, .iqy, .thmx, .sxi
Аудио	.a52, .bin, .cda, .m3u, .wav, .wma, .mp3, .mid, .aac, .mp4, .asf, .mpga, .flac, .ogg, .ra, .w64, .m4a, .m4r, .midi, .aif, .aiff, .mp2
Изображение	.pdf, .svg, .gif, .jpg, .png, .webp, .wmf, .tiff, .tif, .emf, .jpg
Исполняемые файлы Linux	.bin, .elf, .pl, .sh
Исполняемый файл Android	.apk, .jar, .img, .dex, .so
Исполняемый файл Windows	.hta, .jar, .msu, .thm, .exe, .msi, .bat, .cmd, .com, .wsf, .lnk, .dll, .sys, .paf.exe, .scr
Файл реестра Windows	.reg
HTML	.html, .json, .rss, .svg, .xhtml, .shtml, .htm
XML	.kml, .rss, .svg
Почтовые файлы	.eml, .msg, .pst
Скриптовые файлы	.py, .js, .jse, .cgi, .cpp, .json, .kml, .pl, .ps1, .psc1, .sh, .rss, .vbs, .vbe, .pickle
Видеофайлы	gifv, .mng, .asx, .bin, .dat, .wm, .avi, .mpeg, .mp4, .wmv, .mpg, .swf, .3gp, .3g2, .mkv, .webm, .asf, .ts, .rm, .flv

Режим работы

Система ATHENA имеет два режима работы: автоматический и экспертный.

Автоматический режим заключается в перехвате и проверке файлов из интернет-трафика, почтовых вложений, мобильных устройств и API.

Экспертный режим позволяет пользователю детально настраивать динамическую среду по интересующим его направлениям исследования, включая:

- Загрузку вручную любых файлов в систему, в т.ч. посредством telegram-bot
- Настройку параметров исследования и запуск файла
- Наблюдение за исследованием
- Участие в имитации работы пользователя в «песочнице»

Производительность проверки в час

Письма	30 000	60 000	300 000	650 000
Ссылки	500	1 500	5 000	12 000
Файлы	2 000	4 000	5 000	12 000
CPU	16 ядер	32 ядра	48 ядер	64 ядра
RAM	48 GB	64 GB	96 GB	128 GB
SSD	0,5 TB	1 TB	2 TB	4 TB
HDD	2 TB	4 TB	6 TB	10 TB



Проверка до 3 миллионов писем в сутки на одну инсталляцию с возможностью масштабирования

Система AVSOFT ATHENA поддерживает установку на следующих видах операционных систем

- Debian 12

- Astra Linux 1.7

- Ubuntu 22.04