ЕВРАЗ

Нужен ли EDR? Или качественно зафиксированный пациент в анестезии не нуждается

Нуйкин Андрей

10.2023

Что такое ЕВРАЗ?

ЕВРАЗ является вертикально-интегрированной металлургической и горнодобывающей компанией с активами в России, США, Канаде и Казахстане. Компания входит в число крупнейших производителей стали в мире. Собственная база железной руды и коксующегося угля практически полностью обеспечивает внутренние потребности ЕВРАЗа.

Интернет-магазин металлопродукции Evraz.Market

Немного о себе

ЕВРАЗ

•Окончил Военный институт правительственной связи в Орле.
•Некоторое время работал в ФАПСИ.
•Более 20 лет занимаюсь вопросами обеспечения информационной безопасности.
•Член Ассоциации руководителей служб информационной безопасности (АРСИБ), участник БИП-Клуба и КУБИТ.
•С 2010 г. — обладатель международных сертификатов Certified information security manager, Certified information security auditor, Certified in risk and information systems control от организации ISACA.
•За это время работал в различных компаниях в разных областях экономики (банки, ритейл, промышленность и др.): «Евроцемент», «Промсвязьбанк», SELA и др.
•С 2014 г. — начальник отдела обеспечения безопасности информационных систем в компании «Евраз».

Андрей Нуйкин
CISA, CISM, CRISK
АРСИБ
RuSCADASec Coin #29

Отказ от ответственности

Данная презентация является частным мнением и может не совпадать с мнением других организаций и экспертов.

Данное исследование не является окончательным и не ставит целью дискредитацию решений или подходов.

Исследование не охватывает всех продуктов и методик.

Полученные результаты являются не окончательными и требуют дальнейшего всестороннего изучения и сравнения с другими решениями.

Текущая реальность

ЕВРАЗ

- Количество атак неуклонно растет.
  За 2022 год количество атак выросло в 2-3 раза

- Атаки усложняются.
  Применяются все более сложные схемы

- Защищаться сложнее.
  Средства защиты требуют все более тонкой и сложной настройки

Текущая реальность

ЕВРАЗ

- Многие компании активно продвигают решения EDR\XDR

  Решение презентуется как очень эффективное и современное. И если его не внедрить, то наступит всеобщая катастрофа.

- Стоимость решений EDR\XDR высока

  При этом стоимость решения зачастую превышает стоимость антивирусного программного обеспечения и других средств защиты.

- Дополнительный агент\нагрузка

  Само решение требует установку еще одного агента на компьютер. А на нем уже есть много других агентов…

Текущая реальность

ЕВРАЗ

Возникают вопросы:

- А так ли хороши EDR\XDR?
- В какой инфраструктуре они более эффективны?
- Насколько они повышают общую защищенность?

Текущая реальность

ЕВРАЗ

Возникают мысли:

- А есть ли альтернативная защита?
- Возможно правильная настройка Windows решит все проблемы….
- Или наличие мощного современного антивирусного решения достаточно…..
- А еще у нас есть Центр мониторинга…..

Что сделали?

ЕВРАЗ

Возникла мысль проверить эффективность EDR\XDR решений.
Поделился этой мыслью с сообществом и откликнулись коллеги из компании AXXTEL. Коллеги подготовили стенд состоящий из нескольких компьютеров с различной конфигурацией Windows:

- Default Windows + KES
- Default Windows + KEDR
- Windows Hardening Admin (учетная запись имеет административный доступ)
- Windows Hardening NoAdmin (учетная запись не имеет административный доступ)

В качестве средства защиты коллеги выбрали решение Лаборатории Касперского. Хотя это не принципиально. Интересно было бы с любым решением.

Что сделали?

ЕВРАЗ

Далее, были проведены настройки систем

- Windows Hardening Admin (учетная запись имеет административный доступ)
- Windows Hardening NoAdmin (учетная запись не имеет административный доступ)

в соответствии с политиками принятыми в ЕВРАЗ.

К настроенным компьютерам применили 30 различных хакерских техник.

На следующих слайдах будут показаны результаты.

Результат

ЕВРАЗ

Id	Наименование теста	Права админа	АВЗ (KES)	KEDR без KES	Харденинг (не адм УЗ)	Харденинг (адм УЗ)
1	OS Credential Dumping: LSASS Memory	Да	Блокируется	Обнаруживается	Блокируется	Выполнено
2	OS Credential Dumping: Dump LSASS.exe Memory using direct system calls and API unhooking	Да	Блокируется	Без обнаружения	Блокируется	Выполнено
3	OS Credential Dumping: Dump LSASS.exe Memory using Windows Task Manager	Да	Блокируется	Обнаруживается	Блокируется	Выполнено
4	Command and Scripting Interpreter. Mimikatz	Да	Блокируется	Обнаруживается	Блокируется	Выполнено
5	OS Credential Dumping: Security Account Manager. Registry dump of SAM, creds, and secrets	Да	Блокируется	Обнаруживается	Блокируется	Выполнено
6	OS Credential Dumping: DCSync (Active Directory)		Необходимы привилегии доменного администратора			
7	Remote System Discovery. Adfind - Enumerate Active Directory Computer Objects	нет	Выполнено	Обнаруживается. Средняя важность	Выполнено	Выполнено
8	Obfuscated Command in PowerShell	нет	Выполнено	Обнаруживается. Низкая важность	Выполнено	Выполнено
9	HTML Smuggling Remote Payload	Да	Блокируется	Обнаруживается. Низкая важность	Загрузка не блокируется	Загрузка не блокируется

Результат

ЕВРАЗ

Id	Наименование теста	Права админа	АВЗ (KES)	KEDR без KES	Харденинг (не адм УЗ)	Харденинг (адм УЗ)
10	Network Service Scanning. Port Scan Angry IP Scanner	нет	Выполнено	Без обнаружения	Харденинг не применим	Харденинг не применим
11	Network Service Scanning. Port Scan NMap for Windows	нет	Выполнено	Без обнаружения	Харденинг не применим	Харденинг не применим
12	Exfiltration Over Alternative Protocol. DNSExfiltration	нет	Выполнено	Без обнаружения	Харденинг не применим	Харденинг не применим
13	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol. ICMP	нет	Выполнено	Без обнаружения	Харденинг не применим	Харденинг не применим
14	Scheduled Task Executing Base64 Encoded Commands From Registry	нет	Блокируется	Обнаруживается. Средняя важность	Выполнено	Выполнено
15	Process Injection: Asynchronous Procedure Call. Process Injection via C#	нет	Блокируется	Без обнаружения	Выполнено	Выполнено
16	Process Hollowing	нет	Блокируется	Без обнаружения	Выполнено	Выполнено
17	Command and Scripting Interpreter: PowerShell. Run BloodHound from local disk	нет	Выполнено	Обнаружены артефакты. Средняя важность.	Выполнено	Выполнено

Результат

ЕВРАЗ

Id	Наименование теста	Права администратора	АВЗ (KES)	KEDR без KES	Харденинг (не адм УЗ)	Харденинг (адм УЗ)
18	Command and Scripting Interpreter: PowerShell. Obfuscation Tests	нет	Блокируется	Обнаруживается. Средняя важность	Заблокировано. Запрет powershell легко обходится	Заблокировано. Запрет powershell легко обходится
19	Create local account with admin privileges	да	Выполнено	Обнаруживается. Средняя важность	Требуются права администратора	Выполнено
20	System Information Discovery	нет	Выполнено	Обнаруживается. Средняя важность	Выполнено	Выполнено
21	System Information Discovery. winPEAS	нет	Блокируется	Обнаруживается. Средняя важность	Выполнено	Выполнено
22	Ingress Tool Transfer. certutil download (urlcache)	нет	Блокируется	Обнаруживается. Средняя важность	Выполнено	Выполнено
23	Ingress Tool Transfer. Windows - BITSAdmin BITS Download	нет	Блокируется	Обнаруживается (в журналах событий).	Выполнено	Выполнено
24	Brute Force Password Spray Domain Users	нет	Выполнено	Без обнаружения	Выполнено	Выполнено

Результат

ЕВРАЗ

Id	Наименование теста	Права админа	АВЗ (KES)	KEDR без KES	Харденинг (не адм УЗ)	Харденинг (адм УЗ)
25	Network Share Discovery	нет	Блокируется	Обнаруживается. Kapersky доработали правило. Низкая важность	Заблокировано. Запрет powershell легко обходится	Заблокировано. Запрет powershell легко обходится
26	Steal Web Session Cookie. Steal Firefox and Chrome Cookies (Windows)	нет	Блокируется	Без обнаружения	Выполнено	Выполнено
27	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder. Reg Key Run	нет	Выполнено	Только события в логах. Высокий уровень FP	Выполнено	Выполнено
28	Credentials from Password Stores: Credentials from Web Browsers. LaZagne - Credentials from Browser	нет	Блокируется	Без обнаружения	Выполнено. Требуются права администратора	Выполнено
29	Steal or Forge Kerberos Tickets: Kerberoasting	Да	Блокируется	Обнаруживается	Запущено без блокировки.	Запущено без блокировки.
30	Steal or Forge Kerberos Tickets: AS-REP Roasting	Да	Блокируется	Обнаруживается	Запущено без блокировки.	Запущено без блокировки.

Результат

ЕВРАЗ

- Из 30 техник Windows Hardening NoAdmin закрыл 8 штук.
- Антивирусное решение закрыло 18 штук.
- В сумме Hardening + АВЗ закрыли 20 штук (т.к. несколько техник заблокировано обоими решениями).
- EDR добавил еще 4 выявленных техники, дополнительно к предыдущим решениям.

Результат

ЕВРАЗ

- EDR не произвел WOW эффекта.
- EDR повысила защищенность но не настолько, насколько ожидалось.
- Как мы видим при правильной настройке операционной системы и антивирусном программном обеспечении защищенность достаточно велика.
- По факту подтвердилась старая истина:
  Наиболее эффективна комплексная защита
- Вариант использования:
  Для разной критичности – разные комбинации

Дальнейшие шаги

ЕВРАЗ

- Попробовать решения от других производителей EDR\XDR
- Расширить перечень атакующих техник

ЕВРАЗ

Спасибо за внимание

Андрей Нуйкин
CISA, CISM
АРСИБ
RuSCADASec Coin #29

+7(495) 363-19-60

Andrey.nuykin@evraz.com

www.evraz.com