КИБЕРУГРОЗЫ 2023 ДЛЯ ПРОМЫШЛЕННОГО СЕКТОРА

ROOT LEVEL RESOURCES

Часть 2

ОСНОВНЫЕ ТЕХНИКИ MITRE ATTACK ®

TACTIC	MITRE ID	TECHNIQUE
INITIAL ACCESS	T1190	Exploit Public-Facing Application
	T1566.001	Phishing: Spearphishing Attachment
	T1566.002	Phishing: Spearphishing Link
	T1566	Phishing
	T1078.002	Valid Accounts: Domain Accounts
EXECUTION	T1203	Exploitation for Execution
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1106	Native API
	T1204	User Execution
	T1559	Inter-Process Communication
PERSISTENCE	T1547	Boot or Logon Autostart Execution
	T1574	Hijack Execution Flow
	T1547.002	Hijack Execution Flow: DLL Side-Loading
	T1078.002	Valid Accounts: Domain Accounts
	T1078.003	Valid Accounts: Local Accounts
PRIVILEGE ESCALATION	T1547	Boot or Logon Autostart Execution
	T1574	Hijack Execution Flow
	T1055	Process Injection
	T1548	Abuse Elevation Control Mechanism
	T1547.002	Hijack Execution Flow: DLL Side-Loading
DEFENSE EVASION	T1027	Obfuscated Files or Information
	T1140	Deobfuscate/Decode Files or Information
	T1574	Hijack Execution Flow
	T1562	Impair Defenses
	T1036	Masquerading
CREDENTIAL ACCESS	T1552.001	Unsecured Credentials: Credentials In Files
	T1555.003	Credentials from Password Stores: Credentials from Web Browsers
	T1056	Input Capture
	T1003.001	OS Credential Dumping: LSASS Memory
	T1003.003	OS Credential Dumping: NTDS
DISCOVERY	T1082	System Information Discovery
	T1057	Process Discovery
	T1087	Account Discovery
	T1135	Network Share Discovery
	T1069	Permission Groups Discovery
LATERAL MOVEMENT	T1210	Exploitation of Remote Services
	T1570	Lateral Tool Transfer
	T1550.002	Use Alternate Authentication Material: Pass the Hash
	T1021.001	Remote Services: Remote Desktop Protocol
COLLECTION	T1560.001	Archive Collected Data -> Archive via Utility
	T1005	Data from Local System
	T1560	Archive Collected Data
	T1119	Automated Collection
	T1602	Data from Configuration Repository
COMMAND AND CONTROL	T1105	Ingress Tool Transfer
	T1071.001	Application Layer Protocol: Web Protocols
	T1102	Web Service
	T1071	Application Layer Protocol
	T1573.002	Encrypted Channel: Asymmetric Cryptography
EXFILTRATION	T1041	Exfiltration Over C2 Channel
	T1020	Automated Exfiltration
	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage
	T1537	Transfer Data to Cloud Account
	T1485	Data Destruction
	T1489	Service Stop

Спецслужбы, атакующие промышленный сектор

ROOT LEVEL RESOURCES

Мишенью традиционных хакеров, а также для конкурирующих компаний и стран, занимающихся корпоративным шпионажем, все чаще становятся производители. Мотивы таких атак варьируются от финансовой выгоды и мести до конкурентной разведки с целью стратегического прорыва.

Существующие производственные системы разрабатывались, когда кибербезопасность не считалась важной проблемой и основное внимание в производственных технологиях уделялось производительности и безопасности производства (не в информационном ключе). В результате чего и образовались большие пробелы в безопасности. Растущая сложность таких систем привела к созданию сложных и крупных сетевых, узко специализированных инфраструктур. В большинстве случаев эти системы эксплуатируются и управляются не ИТ-специалистами, а специалистами-производителями.

Эти тенденции, в сочетании с интеграцией ИТ и операций, создали большую площадь для атаки, которой очень сложно управлять и защищать.

APT41

Эта сложная вредоносная кампания оставалась незамеченной, как минимум, с 2019 года. Нацелена она была на технологические и **производственные компании** в Северной Америке, Европе и Азии. За годы разведки и выявления ценных данных, этой хакерской группе удалось украсть сотни гигабайт информации.

Под их прицелом оказалась интеллектуальная собственность, разработанная жертвами, включая конфиденциальные документы, диаграммы, формулы, чертежи и конфиденциальные данные, связанные с производством.

Так же они собирали информацию, которая может быть использована для будущих кибератак, например: сведения о бизнес-подразделениях целевой компании, сетевой архитектуре, учетных записях и учетных данных пользователей, электронной почте сотрудников и данных клиентов.

Специалисты, с высокой степенью уверенности, приписывают атаку и операцию **CuckooBees** группе **APT41**.

Первоначальная точка входа в организации возникла из-за многочисленных уязвимостей в организационной платформе планирование ресурсов предприятия (ERP).

Во время атаки злоумышленники использовали новый кастомный руткит – **WINNKIT**. Его цель – действовать как агент в режиме ядра, взаимодействуя с агентом пользовательского режима и перехватывая запросы TCP/IP, обращаясь непосредственно к сетевой карте.

Dark Halo

Весной 2022 на VirusTotal из Шри-Ланки был загружен файл под видом резюме Roshan_CV.iso и содержащий вредоносную нагрузку, связанную с новым инструментом **Brute Ratel C4 (BRc4)** (дата компиляции – 17 мая 2022). Следует обратить внимание, что ни одно антивирусное средство не квалифицировало данный файл как вредоносный.

Специалистам удалось раскрыть часть инфраструктуры и образцов BRc4. Кроме того, установлено, что в Северной и Южной Америке как минимум 3 организации были подвержены воздействию этого инструмента. В том числе **крупный производитель текстиля в Мексике.**

Образец загружался по той же схеме, которую использовала группа **DarkHalo** для распространения Cobalt Strike на машины жертв в последних атаках. Цепочку выполнения атаки можно представить в виде схемы:

Roshan_CV.ISO → Roshan-Bandar_CV_Dialog. LNK → cmd.exe → OneDriveUpdater.exe → version.dll → OneDrive.Update

Конечный код, загруженный в память, представляет собой инструмент Brute Ratel C4.

Lazarus

Северокорейская группа **Lazarus** использовала пейлоады в KMSAuto и троянизированный KeePass для своих изощренных атак.

Весной 2022 произошла **атака на поставщика промышленного оборудования** на Филиппинах, где использовалась похожая троянизированная вредоносная программа KeePass[1].

Цель данной программы – загрузить зашифрованный Mimikatz из файловой системы, для чего требовалось три параметра:

- Расположение зашифрованного Mimikatz в файловой системе
- Ключ для его расшифровки
- Дважды закодированный в base64 аргумент для Mimikatz, который может выглядеть как *privilege::debug,lsadump::dcsync/domain:<DOMAIN>/all /csv.*

Специалисты относят эти файлы к набору специфических инструментов Lazarus.

Осенью 2022 эксперты обнаружили, что Lazarus установили одну из своих полезных нагрузок в *C:\ProgramData\KMSAutoS\KMSAuto.bin* и замаскировали ее под известный инструмент активации Windows.

Полезная нагрузка – это исполняемый файл VMProtect, а не KMSAuto.

Филиппинский поставщик, о котором мы упоминали в связи с троянизированным приложением KeePass также стал жертвой этой нагрузки. Хакеры воспользовались кряком, уже присутствующим в системе жертвы в той же папке, которую обычно предписывают исключить из антивирусной проверки. Так, для безопасности - пиратство – это не только риск доставки ВПО, но и уклонение от обнаружения.

APT40

Не сбавляют обороты и продолжают атаки на различные организации Австралии китайские прогосударственные хакеры **APT40**. Смешение целей, связанных с делами правительства Австралии, а также с производством энергии на шельфе в Южно-Китайском море произошло в последней кампании. Жертвами стали **мировые производители тяжёлой промышленности**, которые проводят техническое обслуживание парка ветряных турбин в Южно-Китайском море.

Производители получали в фишинговых электронных письмах URL-адреса, которые перенаправляли их на вредоносный веб-сайт, выдающий себя за австралийское новостное агентство. В свою очередь, целевая страница веб-сайта доставляла вредоносный код JavaScript ScanBox[2] своим целям.

В единичных случаях ScanBox доставлялся с веб-сайтов, которые подвергались атакам стратегической веб-компрометации (SWC), когда на законные сайты внедрялся вредоносный код JavaScript. Таким образом злоумышленник контролирует вредоносный сайт и доставляет вредоносный код пользователям.

Aggah

Летом 2022, группа **Aggah** производились фишинговые рассылки на промышленные организации Тайваня и Южной Кореи.

Одна из рассылок проводилась от имени компании по доставке еды FoodHub. Письмо содержало информацию о заказе и вложение Purchase order 4500061977,pdf.ppam. Получателем была тайваньская компания Fon-Star International Technology Inc.

Другими жертвами подобных писем стали:

- **CSE group** – Тайваньская мануфактура
- **FomoTech** – Тайваньская инжиниринговая компания
- **Hyundai Electric** – Корейская энергетическая компания

Отправленное вложение содержало обфусцированный макрос, который использует MSHTA, чтобы выполнить Jscript, размещённый на скомпрометированном легитимном сайте индийского отеля.

На WordPress находилось большинство легитимных скомпрометированных сайтов, используемых для размещения вредоносной нагрузки. Jscript проверяет факт использования средств отладки, после чего происходит обращение по другому скомпрометированному сайту афганской компании по доставке еды.

Сначала хакеры загружают и исполняют скрипт PowerShell, который используется для проверки статуса антивирусных средств (проверяется наличие Windows Defender, ESET, или их отсутствие. По результатам чего будут использоваться разные загрузчики для инжектирования Warzone[3] в легитимный процесс.

Tropic Trooper

При атаках на финансовые организации и **производственные компании** группа использует xPack.

Данный бэкдор позволяет хакерам удаленно запускать команды WMI и монтировать общие ресурсы через SMB для передачи им данных с серверов C&C. Злоумышленники также использовали ВПО для просмотра веб-страниц в качестве прокси-сервера для маскировки своего IP-адреса.

Одна из атак, проведенных группой, оставалась в скомпрометированной сети производственной организации Тайваня **в течение 175 дней**.

В настоящее время первоначальный вектор заражения неясен. Специалисты предполагают, что хакеры использовали веб-приложение или службу, поскольку в одной из атак служба MSSQL применялась для выполнения системных команд.

Exforel

Китайский **Daxin** оставался **в тени более 10 лет**. Специалисты по безопасности обнаружили развертывание данного инструмента в государственных организациях, а также в организациях телекоммуникационного, транспортного и **производственного секторов**.

Daxin поставляется в виде редкого формата для вредоносных программ - драйвера ядра Windows. Он реализует расширенные коммуникационные функции, которые обеспечивают высокую степень скрытности и позволяют коммуницировать с зараженными компьютерами в высокозащищенных сетях, **где недоступно прямое подключение к Интернету**.

Daxin также может передавать свои сообщения по сети зараженных компьютеров в атакуемой организации. Злоумышленники могут выбрать произвольный путь через зараженные компьютеры и отправить команду предлагающую установить запрошенное соединение.

ВПО избегает запуска собственных сетевых служб. Взамен оно злоупотребляет законными службами работающими на зараженных компьютерах.

ROOT LEVEL RESOURCES

ПРОГНОЗЫ

Количество атак со стороны шифровальщиков будет расти

- В качестве точки входа для атак все чаще будут использоваться компьютеры инженеров и разработчиков ПО, поскольку они предоставляют доступ к системам АСУ ТП и обладают повышенными привилегиями.
- Эксплуатация старых уязвимостей, в том числе касающихся роутеров, продолжит оставаться главным вектором атаки, так как не все компании проактивно устанавливают патчи безопасности.
- Ожидается рост числа атак на цепочки поставок и атак через доверительные отношения (trusted relationship attack), когда хакеры получают доступ к производствам через компрометацию поставщиков ПО или телекоммуникационных услуг.

1 KeePass — это бесплатный менеджер паролей с открытым исходным кодом, который помогает пользователю безопасно управлять своими паролями.

2 ScanBox Primer: ScanBox – это платформа веб-разведки и эксплуатации на основе JavaScript, которая позволяет злоумышленникам профилировать жертв и доставлять ВПО выбранным интересующим целям.

3 Warzone RAT – информационный C++ стилер, поддерживающий возможности повышения привилегий, кейлогинг, Remote Shell, загрузку и выполнение файлов, работу с файлами, обеспечение персистентности, кражу учетных данных.