Целевые атаки на промышленные ИС

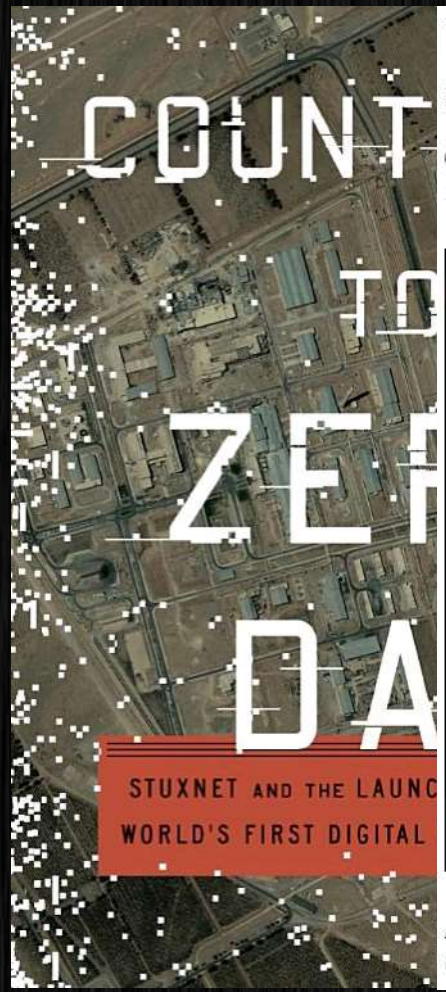
Легезо Денис
Лаборатория Касперского

E-mail: Denis.Legezo@Kaspersky.com
Facebook: Denis Legezo
Twitter: @legezo

План на ближайшие 20 минут

- Известные инциденты
- Эксперимент по получению контроля над АСУТП
- Проще начинать с людей
- Разбор APT Crouching Yeti
- Что мешает обнаружению атак?

Инциденты именно с АСУТП



Hack attack causes ' steel works

22 December 2014 | Technology

The hack attack led to failures in plant equipment a

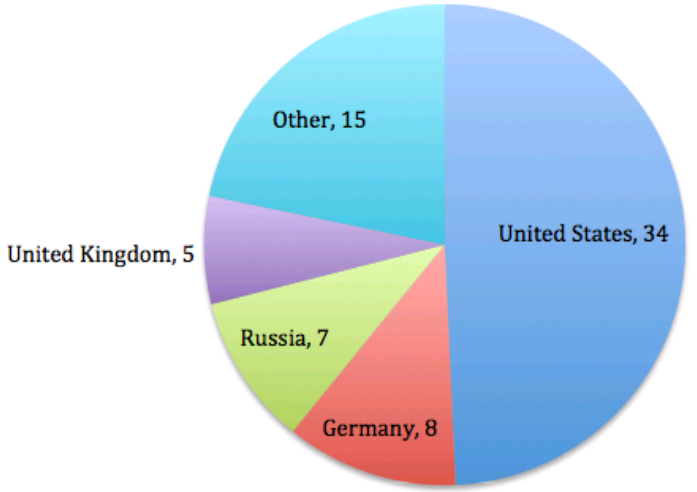
A blast furnace at a German steel mill suffi
cyber attack on the plant's network, says

SECURELIST THREATS CATEGORIES TAGS ENCYCLOPEDIA

C2 and victims:

Overall, we successfully monitored **69** C2 server (unique domains), receiving hits from **3699** victims (unique IDs of the Trojan/backdoor) connecting from **57796** different IP addresses. We gathered four additional C2s since the publication of the first report (65 in the last report).

C2 country distribution



Инциденты с промышленными ИС

- Инцидентов на самом деле гораздо больше
- Практически все APT затрагивают промышленные объекты
- Многие продвинутые APT научились успешно преодолевать air gap (Turla, MiniDuke, RedOctober, …)
- Защиты на хосте недостаточно, но она обязательно должна там быть

Эксперимент

Цель: выяснить, возможно ли получить полное управление АСУТП

- Используя только общедоступные и бесплатные средства
- Без 0-day и разработки новых эксплоитов
- Профессионалу ИБ, не разбирающемуся в АСУТП

Тестовый стенд:

- рабочие станции под управлением Windows XP
- с развернутой Siemens PCS7 (WinCC и STEP 7)
- ПЛК Siemens S7-317 и два S7-414
- Ethernet и PROFIBUS, Siemens SCALANCE X-200/300 Ethernet switches
- сегментация сети с помощью firewall Siemens SCALANCE S-612, все АСУ-устройства во внутренней сети

Придаем реальности: конфигурация «как установил подрядчик»

- отсутствуют требования к паролям
- отсутствует IDS
- отсутствуют обновления
- нет средств управления конфигурациями

Средства для атаки:

- Kali Linux
- Metasploit
- NMap
- командная строка Linux

- Шаг 1: сканируем nmap-ом сеть снаружи, обнаруживаем файрволл и рабочую станцию
- Шаг 2: сканируем nmap-ом все порты рабочей станции, обнаруживаем SNMP с конфигурацией «по умолчанию» (пароль – «password»)
- Шаг 3: через SMTP nmap-ом получаем информацию о версии ОС (Windows XP SP3), ее пользователях, запущенных сервисах и процессах, общих папках, установленном ПО и обновлениях
- Среди сервисов обнаруживается Microsoft SQL Server 2005 с БД WINCC, на нестандартном порту 1031 (вместо 1433)

- Шаг 4: сканируем Metasploit-ом SQL Server, обнаруживаем включенные опции «remote access» и «xp_cmdshell».
- Шаг 5: с помощью Hydra брутфорсим пароль для учетной записи SQL «Administrator», это оказывается «Administrator»
- Шаг 6: с помощью Metasploit запускаем модуль mssql_payload, загружающий через xp_cmdshell модуль Meterpreter – удаленную command-line консоль управления. Крадем хэши паролей Windows.
- Шаг 7: с помощью встроенных модулей Metasploit включаем для себя Remote Desktop. Теперь мы можем видеть HMI, который, однако, здесь (во внешней сети) ничем не управляет

- Шаг 8: после внимательного осмотра рабочей станции обнаруживаем на ней конфигурационные файлы файрволла Siemens SCALANCE S-612, и утилиту для его настройки. Сам Siemens рекомендует настраивать файрволл из внешней сети (Siemens AG 2005).
- Даже если бы конфигурационные файлы мы не обнаружили, этот файрволл подвержен брутфорсу (ICS-CERT 2012).
- Шаг 9: Логинимся на файрволл, открываем доступ во внутреннюю сеть.
- Шаг 10: С помощью Metasploit осуществляем ARP-сканирование внутренней сети, получаем список всех устройств

- Шаг 11: использую полученную ранее на рабочей станции учетную запись Administrator из Windows подключаемся к компьютерам во внутренней сети.
- Шаг 12: Получаем полный контроль над тех. процессом через WinCC Explorer или WebNavigator

Проще начинать с людей

Павел Матюшин — люблю работу на переднем фронте R&D
начальник отдела, ОАО "**Концерн "Созвездие"**, Воронеж, 1997 — н.в..
Россия, Воронежская область, Воронеж.

за 3-м кругом

Туяна Вискова (Тужинова) — программист
ведущий инженер-конструктор, ОАО "**Концерн "Созвездие"**, Воронеж, 2009 — н.в..
IT, интернет, связь, телеком / Программирование, разработка, тестирование; Россия, Воронежская область, Воронеж.

за 3-м кругом

Герман Долгун — инженер
инженер, Воронежский НИИ связи ныне "**Концерн" Созвездие"**, Воронеж, 2003 — н.в..
IT, интернет, связь, телеком / Системное администрирование, БД; Россия, Воронежская область, Воронеж.

за 3-м кругом

Александр Медведев
Специалист в области метрологического обеспечения производства, **Концерн Созвездие**, Воронеж, 2007 — н.в..
Производство / Радиоэлектронная промышленность; Россия, Воронежская область, Воронеж.
пригласить в 1-й круг

за 3-м кругом

Савченко Сергей
Начальник Службы экономической безопасности, ОАО "**Концерн "Созвездие"**, Воронеж, 1995 — н.в..
Россия, Воронежская область, Воронеж.

inj3ct0r

Inj3ct0r is the ultimate database of exploits and vulnerabilities and a great resource for vulnerability researchers and security professionals.
Our aim is to collect exploits from submittals and various mailing lists and concentrate them in one, easy-to-navigate database.
This was written solely for educational purposes. Use it at your own risk. The author will be not responsible for any damage. // r0073r

[win32]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK				-::GOLD	-::AUTHOR
2013-04-21	Windows7 Disable Task Manager Shellcode - 326 chars	win32	10875		R	D	!	free	Ayrbyte
2013-04-21	Windows7 Force Shutdown Shellcode - 215 chars	win32	6549		R	D	!	free	Ayrbyte
2013-04-21	Windows7 Force Terminate Explorer Shellcode - 255 chars	win32	4397		R	D	!	free	Ayrbyte
2013-03-08	Windows7 Sub_Xor MessageBox Exec Shellcode - 265 Bytes	win32	6333		R	D	✓	free	KedAns-Dz
2012-11-05	win32/xp sp3 - Full ROP calc shellcode	win32	4618		R	D	✓	free	b33f
2012-07-03	win32/7 Ultimate MessageBox ShellCode	win32	3509		R	D	!	free	Ayrbyte
2012-06-10	win32/Seven Ultimate calc.exe ShellCode	win32	4358		R	D	!	free	Ayrbyte
2012-06-08	win32/Seven Ultimate mspaint.exe ShellCode	win32	2275		R	D	!	free	Ayrbyte
2012-02-15	win32/xp sp2 ARABIC (ar) backconnect + acceptconnection 376 bytes	win32	3056		R	D	!	free	TrOoN
2012-02-03	win32/xp sp2 ARABIC (ar) mechanism shellcode + proxy 500 bytes	win32	2172		R	D	!	free	TrOoN
2012-01-29	win32/xp sp2 ARABIC (ar) Message Box Shellcode (87 bytes)	win32	2027		R	D	!	free	TrOoN
2012-01-29	win32/xp sp3 (ENG) cmd.exe Sellcode 87 bytes	win32	3115		R	D	!	free	TrOoN
2011-07-23	win32 / Windows7 Sp1 - rename .jpeg to .vir - 57 bytes	win32	5083		R	D	!	free	TheUzuki

лучшая статья

От кого: **Сосанна Белая** <bsosanna@mail.ru>

Кому: [redacted]

28 июля 2012, 06:55 1 файл

Если вы умный человек, то после того как вы прочитали эту статью, вы не могли бы помочь, но переслать её своим друзьям.
Чтение - умение.

Все файлы проверены, вирусов нет

Прикрепленные файлы: 1

лучшая статья.doc

253 КБ Посмотреть Скачать

Быстрый ответ Ответить всем Переслать


How a watering hole technique works:
Attacker injects exploit into selected sites often visited by targeted victims.
Exploit drops the malware onto vulnerable systems.
Using the dropped malware, the attacker may now initiate his malicious activities
Attacker gathers initial intelligence to determine which sites to target.

Energetic Bear / Crouching Yeti

- APT с 2010 года, более 2800 жертв
- Энергетика, машиностроение, промышленность и фармацевтика
- Распространение через
  - письма с экплоитом
  - зараженные легитимные сайты (watering hole)
  - переупакованные и зараженные легитимные инсталляторы
- Взломанные легитимные сайты в качестве командных центров
- Применение нескольких различных троянских программ, бэкдоров, и эксплоит-паков

- Скомпрометированные инсталляторы на сайтах производителей:
  - "eWon" - Бельгийский производитель SCADA и промышленного сетевого оборудования
  - "MB Connect Line GmbH" - компания, выпускающая ПО для удаленного управления ПЛК
  - "MESA Imaging" - производитель сверхскоростных 3D-камер и сенсоров

- Примеры скомпрометированных ресурсов для watering hole:
  - gse.com.ge - Georgian State Electrosystem
  - gamyba.le.lt - Lithuania‘s largest electricity generating company
  - chariotoilandgas.com - Chariot Oil and Gas Ltd
  - longreachoilandgas.com - Longreach Oil & Gas Ltd
  - vitogaz.com - French-based gas distributor, supplier and technical developer

- Порты, используемые плагином Havex для обнаружения OPC :
  - 502 - Modbus
  - 102 - Siemens PLC
  - 11234 - Measuresoft ScadaPro
  - 12401 - 7-Technologies IGSS SCADA
  - 44818 - Rockwell Rslinx / FactoryTalk

aluigi.altervista.org/adv.htm

Luigi Auriemma

me@aluigi.org

ADVISORIES

The complete archive of my advisories about software security vulnerabilities found by me.
The (SCADA) tag covers anything of the HMI/SCADA, PLC, automation and industrial sector.
There are other tags like (enterprise), (game), (media), (streaming), (p2p) and (no tag) for other types of software.
All the advisories include the steps for replicating the problems or links to the relative proof-of-concept.

Heap overflow in Rockwell RSLogix 19 (FactoryTalk RnaUtility.dll) (SCADA)
13 Sep 2011: adv - rslogix_1

Multiple vulnerabilities in Measuresoft ScadaPro 4.0.0 (SCADA)
13 Sep 2011: adv - scadapro_1

Vulnerabilities in 7-Technologies IGSS 9.00.00.11059 (SCADA)
21 Mar 2011: adv1 - adv2 - adv3 - adv4 - adv5 - adv6 - adv7 - adv8 - igss_1/8

Vulnerabilities in DATAC RealWin 2.1 (Build 6.1.10.10) (SCADA)
21 Mar 2011: adv1 - adv2 - adv3 - adv4 - adv5 - adv6 - adv7 - realwin_2/8

- Отчет US ICS-CERT (ICSA-14-178-01) :
  - In particular, the payload gathers server information that includes CLSID, server name, Program ID, OPC version, vendor information, running state, group count, and server bandwidth. In addition to more generic OPC server information, the Havex payload also has the capability of enumerating OPC tags.
  - ICS-CERT testing has determined that the Havex payload has caused multiple common OPC platforms to intermittently crash. This could cause a denial of service effect on applications reliant on OPC communications.

== ping of death

Проблемы обнаружения

- Отсутствие сетевого мониторинга
- Отсутствие экспертизы во вредоносном ПО
  - Любая неполадка списывается на «вирус»
  - Заражение неизвестным вредоносным ПО трудно обнаружить без привлечения сторонних экспертов
- Проще переустановить, чем разбираться
- Файлы от самих SCADA-вендоров не подписаны

Спасибо!

E-mail: Denis.Legezo@Kaspersky.com
Facebook: Denis Legezo
Twitter: @legezo