АКТУАЛЬНЫЕ ВОПРОСЫ АТРИБУЦИИ ЦЕЛЕНАПРАВЛЕННЫХ КИБЕРАТАК

Международная экспертная встреча "Международное сотрудничество по противодействию глобальным угрозам в ИКТ-пространстве: возможности и перспективы», Москва, 22 июня 2021 г.

Алексей Марков,
д.т.н., CISSP,
МГТУ им. Н.Э.Баумана

Предисловие

Повестка дня первой встречи президентов:

МИР

Помощник Байдена рассказал о поднятой им на встрече с Путиным теме кибератак

18 июня 2021, 03:11

2093

ДЖО БАЙДЕН КИБЕРАТАКИ США

Three things to watch as Joe Biden meets Vladimir Putin

BBC

Курьезы: нечеткости дословного перевода ответа на обвинения по теме кибератак («атрибуция по IP-адресу»)

14 июн, 22:18

ТАСС

NBC дословно перевела цитату из "Золотого теленка" в интервью Путина

Большинство фразеологизмов телекомпания перевела буквально, цитаты из хорошо известных в России произведений приводятся без кавычек

План доклада

- Актуальность
- Терминологический аппарат и проблематика
- Экспертные организации и сообщества
- Объект исследования
- Предмет исследования
  - Исследование объективных показателей кибератак
  - Исследование процесса субъективных доказательств
- Предложения по регулированию

I. Актуальность

Объективные факторы:

- Экспоненциальный рост атак и постоянный рост обвинений
- Новые факторы геополитики (в киберпространстве)
  - Атрибуция влияет на общественное мнение
  - Атаки затрагивают экономическое развитие стран («величайшее распределение богатства»)
  - Способность атрибутирования – условие военного и пр. прогноза
- Атрибуция – условие существование ИКТ-отрасли, составная часть анализа угроз (Threat Intelligence), имеет техническое, юридическое и пр. значения
- Рост неравенства в мире - разные возможности у разных стран (геополитические союзы, доступ к магистралям, обладатели облачных технологий, супервычислителей, систем ИИ и пр.)

Субъективный фактор: проблематика обсуждается на самом высоком политическом уровне

II. Понятийный аппарат

- Атрибуция кибератак - термин отсутствует в стандартах и каталогах по безопасности, как-то: IEC, ISO, NIST, ГОСТ, ISACA, BSI (FOIS)

- Атрибуция кибератак - комплекс процедур по выявлению источника атаки с целью **возложения ответственности**

encyclopedia
by Kaspersky

Общий этап атрибуции кибератаки

- Инцидент =>
  - Фиксация ситуации
  - Проведение комплекса циклов экспертизы
    - Сбор данных
    - Анализ данных
    - Оценка полноты данных и достоверности результата
  - Идентификация и возложение ответственности
  - Осуществление контрмер

Уровни атрибуции

Принято разделять на:

- Техническую (криминалистическую), выполняющую функцию определения;
- Политическую (правовую, дипломатическую), выполняющую предписывающую функцию

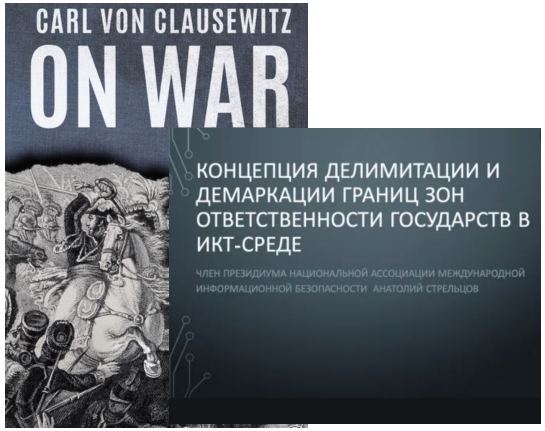
Тип	Функция	Достоверность	Базовые методы	Показатели, критерии
Техническая (криминалистическая)	Определения (детективная)	Высокая	Мониторинг, контроль ресурсов и процессов	Количественные, качественные
Политическая (нормативная, дипломатическая)	Предписывающая	Низкая	Соблюдение норм, анализ мотивации	Качественные (например, highly likely)

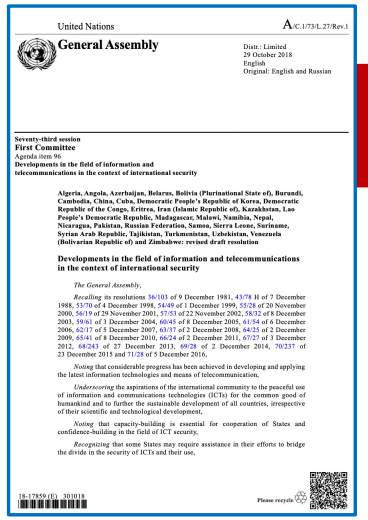
Проблематика атрибуции и кибервойн

Барьеры - в проклятии неопределенности

- Политический уровень (государства)
- Правовой
- Организационно-технический
- Технический уровень
  - Уровень межсетевого взаимодействия (реализации)
  - Системный (программный) уровень (конструирования)
- Иные (человеческий фактор, бизнес и пр.)

- Атаки под «чужим флагом»




United Nations A/C.1/73/L.27/Rev.1

General Assembly

Distr.: Limited
29 October 2018
English
Original: English and Russian

Seventy-third session
First Committee
Agenda item 96
Developments in the field of information and telecommunications in the context of international security

Algeria, Angola, Azerbaijan, Belarus, Bolivia (Plurinational State of), Burundi, Cambodia, China, Cuba, Democratic People's Republic of Korea, Democratic Republic of the Congo, Eritrea, Iran (Islamic Republic of), Kazakhstan, Lao People's Democratic Republic, Madagascar, Malawi, Namibia, Nepal, Nicaragua, Pakistan, Russian Federation, Samoa, Sierra Leone, Suriname, Syrian Arab Republic, Tajikistan, Turkmenistan, Uzbekistan, Venezuela (Bolivarian Republic of) and Zimbabwe: revised draft resolution

Developments in the field of information and telecommunications in the context of international security

The General Assembly,

Recalling its resolutions 36/103 of 9 December 1981, 43/78 H of 7 December 1988, 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012, 68/243 of 27 December 2013, 69/28 of 2 December 2014, 70/237 of 23 December 2015 and 71/28 of 5 December 2016,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Underscoring the aspirations of the international community to the peaceful use of information and communications technologies (ICTs) for the common good of humankind and to further the sustainable development of all countries, irrespective of their scientific and technological development,

Noting that capacity-building is essential for cooperation of States and confidence-building in the field of ICT security,

Recognizing that some States may require assistance in their efforts to bridge the divide in the security of ICTs and their use,

18-17859 (E) 301018

Please recycle

- децентрализованная сегментируемая архитектура мета-сети
- ограничения адресации IPv4
- сервисы по аренде коммуникаций и пр.
- разного рода средства, сервисы и сети анонимизации
- наличие серого и черного рынка вредоносных ресурсов
- небезопасные протоколы (возможность подмены адресации)

- структурная сложность программных ресурсов

Друзья атрибуции

- Субъективный фактор (ляпы, ошибки, мотивы, традиции/ограничения, гордыня.. и пр.)
- Возможные политические, правовые, организационные, технические меры по сквозной подотчетности

III. Исследовательские сообщества

- Спецслужбы (расследование, контрразведка)
- ИБ-организации, специализирующиеся на компьютерных экспертизах
- Академические сообщества
- Национальные и межгосударственные программы

Вопрос о степени объективности?

ИБ-компании: отчеты по атрибуции

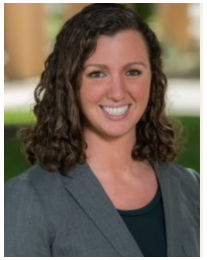
Организация	Страна	Тип организации	Пример интернет-источника
Cisco (Talos)	США	Публичная компания	https://blog.talosintelligence.com/2018/02/group-123-goes-wild.html
CrowdStrike Holdings	США	Публичная компания	www.crowdstrike.com/blog/meet-the-adversaries/
FireEye (Mandiant)	США	Публичная компания	s/apt-
MITRE	США	Некоммерческа организация	
NSA	США	Федеральная служба	www.nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance/
Secureworks (Dell)	США	Публичная компания	www.secureworks.com/research/threat-profiles
Лаборатория Касперского	Россия	Акционерное общество	www.securelist.com/all/?category=908

99% кибероперацій – 10 стран!
Некоторые страны скрывают информацию

Проекты по информированию: Stanford & FD

attribution.news

tools and tips for journalists covering cyberwarfare and info ops

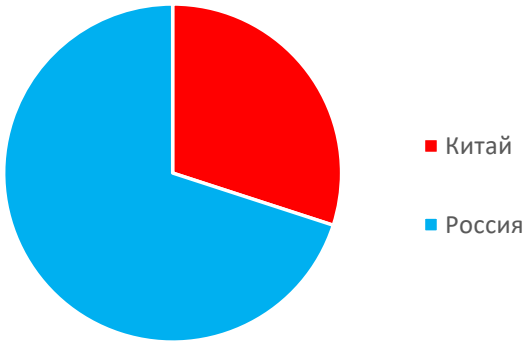





Stanford | Internet Observatory Cyber Policy Center

FIRSTDRAFT

Информирование по Stanford & FD



Национальные и межгосударственные проекты по атрибуции кибератак

Worldwide Observatory of Malicious Behaviors and Attack Threats
project public space

WOMBAT

DARPA-BAA-16-34: Enhanced Attribution | Research | USC

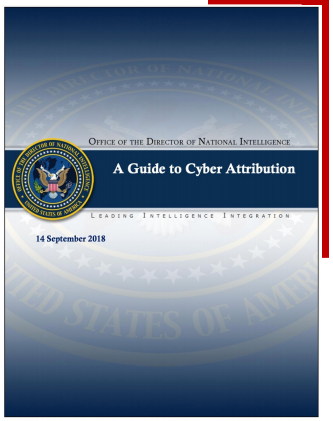
DARPA-BAA-16-34: Enhanced Attribution

Slots:
Proposers may only submit one proposal as lead institution to the Enhanced Attribution program. Each proposal may cover one or more technical areas. Proposers may include additional pages for each technical area addressed in the technical approach

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

› Defense Advanced Research Projects Agency › Our Research ›

Enhanced Attribution



MITRE … Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)

IV. Объект исследования: целенаправленные атаки и APT-группы

130 APT-групп:

- Мотивированы задачами государства

Характеристики APT-атак

Важные характеристики APT-атаки (кибероперации):

- финансируемые государством (+ время, ресурсы, технологическая культура, уязвимости zeroday)
- имеющие этап «эскалации привилегий»

Сопутствующие понятия: killchain (этапность)

Признаки - улики:

- Функциональные
- Структурные
- Информационные (заявления, политические и экономические мотивы, постдействия, демонстрация/маскировка)

V. Предмет исследования: методы атрибуции

- Методы анализа признаков (выявление, оценка значимости признаков, оценка достоверности результата)
- Методы моделирования процесса атрибуции и принятия решения

5.1. Модели криминалистической экспертизы

- Поведенческая модель (техники и тактики атакующих)
- Многофакторная модель
- Приложения ИИ (обучающие системы, технологии нейронных сетей)

Таксономия MITRE: постповеденческий подход

... Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		

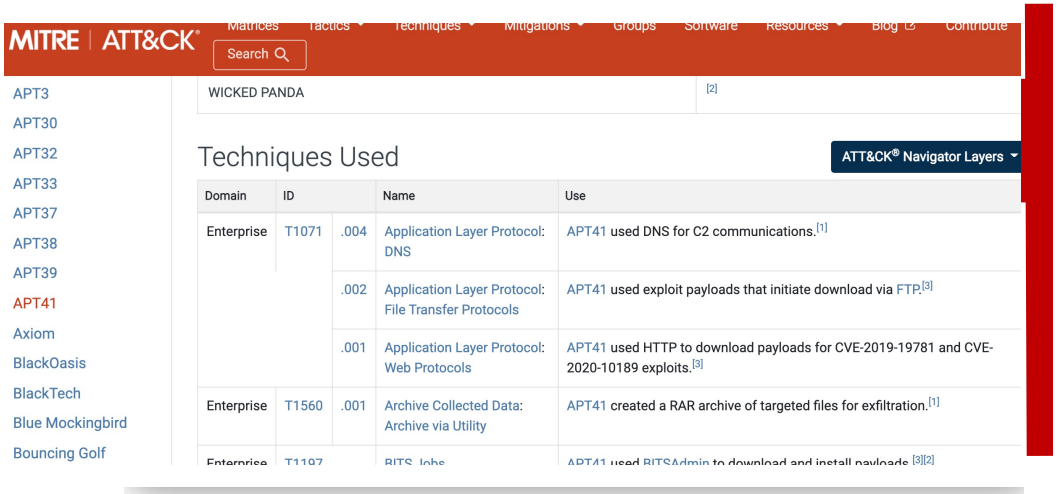
Пример

MITRE ATT&CK

Тактики

- Разведка
- Использование ресурсов
- Первоначальный доступ
- Исполнение
- Настойчивость
- Повышение привилегий
- Уклонение от защиты
- Доступ к учетным данным
- Исследование сети
- Боковое движение
- Сбор данных
- Командование и контроль
- Извлечение данных
- Воздействие

Какие страны представлены?



CARET – Cyber Analytics Repository Exploration Tool

Техники

- Перебор паролей

...

- Дампирование
- ..

- Отгадывание паролей
- Перехват
- Подбор
- Повтор

- /etc/passwd and /etc/shadow
- SAM
- кэши..
- ...

Кстати, атрибуция по версии MITRE

admin@338
APT1
APT12
APT16
APT17
APT19
APT3
APT30
Axiom
BRONZE BUTLER
Deep Panda
Elderwood
Ke3chang
menuPass
Moafee
Naikon
Night Dragon
PittyTiger
Putter Panda
Scarlet Mimic
Suckfly
TA459
Threat Group-3390
Winnti Group

APT28
APT29
Dragonfly 2.0
Sandworm Team
TEMP.Veles
Turla

?

Многофакторный анализ (сигнатуры и аномалии)

A. Особенности программных ресурсов (уязвимости, артефакты и пр.);
B. Особенности сетевой активности (IoC, сетевая инфраструктура);
C. Методические особенности атаки (поведенческие признаки);
D. Данные о субъектах атаки (мотивация группы, психология персонала);
E. Иная информация, полученная без использования собственно компьютерных сетей, например: техническая и агентурная разведка, аналитика по косвенным причинам, разного рода провокации и пр.

Пример классификации и атрибуции кибератак

Название	Уязвимость (A1)	Программы (A3)	Цели (C3)	Источник (B1)	Тактические приемы (C1)	Группа
Атака на посетителей форумов, посвященных исламскому джихаду	Уязвимость в Firefox 17 (TOR Browser)	Неизвестный эксплойт	В список целей не были включены IP-адреса Иордании, Турции и Египта, но были включены пользователи определенного провайдера спутникового интернета в Афганистане.	Серверы, используемые Equation Group	Атаке подвергались только авторизованные пользователи, которые зашли с определенных IP-адресов.	Equation Group
Атака на правительственные организации с использованием уязвимости CVE-2017-11882	Уязвимость в Microsoft Office CVE-2017-11882	Backdoor, написанный на PowerShell-POWRUNER	Правительственные организации в странах Ближнего Востока.	н/д	Массовые рассылки сообщений с использованием скомпрометированных учетных записей. Социальная инженерия.	APT 34

5.2. Модели возложения ответственности

Цели: правдоподобное возложение ответственности

Суть: мозговая атака/структурированный анализ, принятие решения под углом дипломатических задач

Задачи:

- Сбор, анализ данных с целью получения идентификационных признаков
- Принятие решение о возложении ответственности
- Публикация
- Постреакции

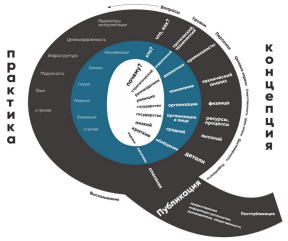
Серые зоны

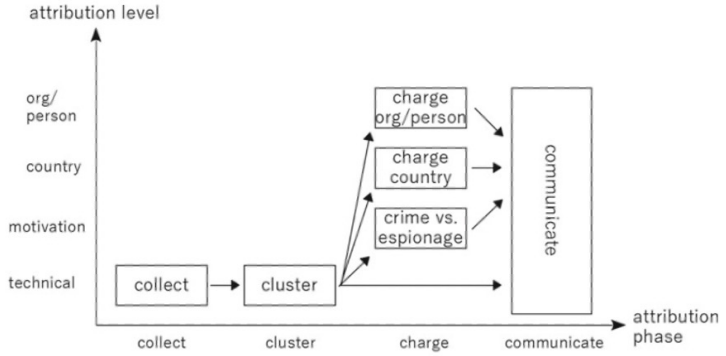
- Отрицание
- Степень ответственности
- Степень ответных действий

- Обвиняемое государство отрицает причастность к компьютерной атаке
- Обвиняемое государство отрицает связь с идентифицированными субъектами атаки, действующими с его территории
- Обвиняющее государство затрудняется обосновать уровень ответных действий (защита, сдерживание, наступательные действия) в киберпространстве
- Обвиняющее государство затрудняется обосновать возможность применения кинетического оружия в ответ на недружелюбные действия в виртуальном пространстве

Примеры концептуальных моделей

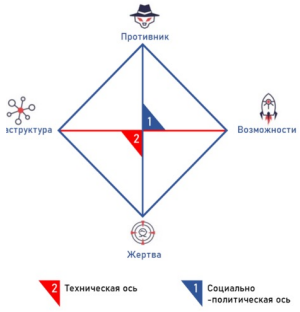
- Q-модель
- MICTIC-модель
- Конкурирующие гипотезы
- Даймонд-модель и ее вариации..
- 4C – модель и пр.



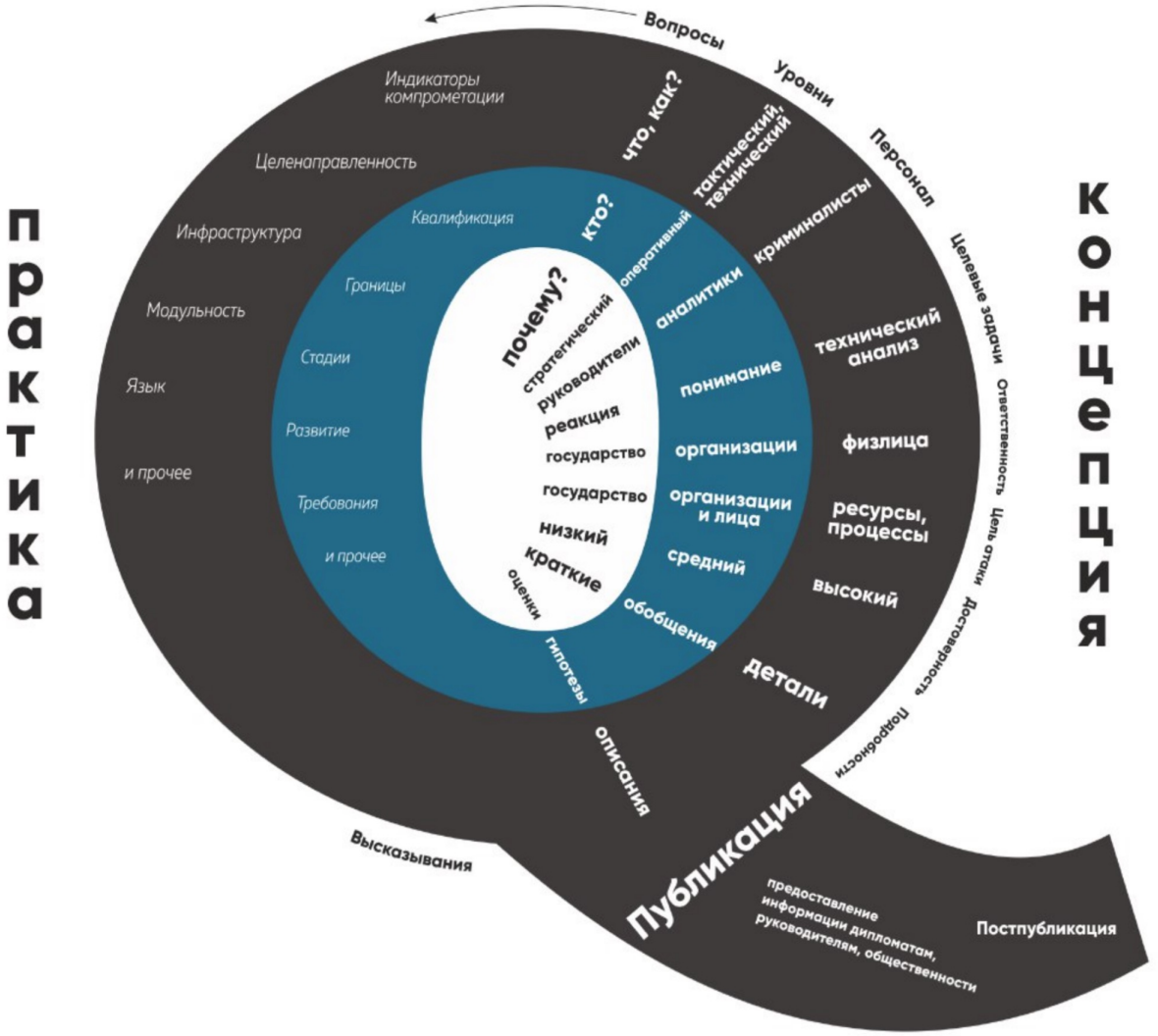


Evidence	Effort	H1	H2	H3	H4	H5	H6	H7
Arabian strings	Low	–	+	–	–	–	–	–
Hindi strings	Low	–	–	–	–	–	+	–
JohnClerk in PDB	Low	–	–	–	–	+	–	–
Spanish lang. res.	Low	–	–	+	–	–	–	–
C&C servers in SK	Med	o	o	o	+	o	o	o
code-sim RedOct.	High	+	–	–	–	–	–	–
targets like RedOct.	High	+	–	–	–	–	–	–
activity in UTC+2	High	+	–	–	–	–	–	–
	Score	2.7	–3.7	–3.7	–3.7	–3.7	–3.7	–4.3

	Aspect
M	Malware
I	Infrastructure
C	Control server
T	Telemetry
I	Intelligence
C	Cui bono



Q-модель: структурированный 3–х уровневый анализ



MICTIC – параллельный подход

M	Malware	Вредоносные программы
I	Infrastructure	Инфраструктура
C	Control server	Сервер управления
T	Telemetry	Отладочные данные
I	Intelligence	Разведка
C	Cui Bono	Кому это выгодно?

Общие выводы

- Актуальность – мир движется в область киберпространства
- Присутствуют как барьеры субъективного (политического) и объективного (интернет) характера, так и улики
- Перекос в сторону Запада
  - Стандарты
  - Группы анализа
  - Информирование
  - Технологические ограничения
- Мир хрупок: надо договариваться
- Вопрос: можно ли регулировать процесс атрибуции?

Связь атрибуции и регулирования ИБ

Решение проблемы атрибуции –>

- Международное сотрудничество в правовом поле (правовое регулирование)
- Международное сотрудничество в нормативной и технической сфере (специальное/техническое регулирование)

Дипломатические направления по повышению эффективности атрибуции

- Выполнение соглашений группы правительственных экспертов ООН
- Осуществление взаимодействия между группами CERT различных стран
- Организация экспертного сообщества исследователей для совместной выработки решений на основе различных интересов и подходов
- Осуществление взаимодействия на политическом и техническом уровнях для расследования инцидентов
- Создание консультационных механизмов для повышения доверия
- Усиление защиты критически важной инфраструктуры
- Международное взаимодействие по обмену информацией об инцидентах, их характерных признаках и степени их угроз
- Соглашение о запрете кибератак на объекты критической информационной инфраструктуры

Организационно-технические направления по повышению эффективности атрибуции

- Использование на узлах информационной инфраструктуры стран модулей, обеспечивающих механизмы подписи данных
- Подпись и децентрализованное хранение журналов
- Дополнение трафика специальной информацией, содержащей подпись наблюдателя
- Передача дополнительных подписанных сообщений о трафике
- Внесение неопределенности для злоумышленника (изменение конфигурации, использование сетевых ловушек, использование водяных знаков, раскрывающих злоумышленника)
- Применение общей распространенной структуры систем обнаружения вторжений с общими актуальными международными базами правил
- Ведение реестра злоумышленников

Thank you for your attention!

Prof. Alexey Markov,
Bauman Moscow State Technical University,
a.markov@bmstu.ru

Литература

Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / Отв. ред. – А.В. Загорский, Н.П. Ромашкина. – М.: ИМЭМО РАН, 2020. – 98 с.

Romashkina N.P., Markov A.S., Stefanovich D.V. International Security, Strategic Stability and Information Technologies – Moscow, IMEMO, 2020. – 98 p. (Rus). DOI: 10.20542/978-5-9535-0581-9.