ПОЛИТЕХ
Институт кибербезопасности и защиты информации

Министерство науки и высшего образования Российской Федерации
Санкт-Петербургский политехнический университет Петра Великого
Институт кибербезопасности и защиты информации

конференция РусКрипто

Защита узлов от распределенного сканирования из сети Интернет

Пахомов М.А.

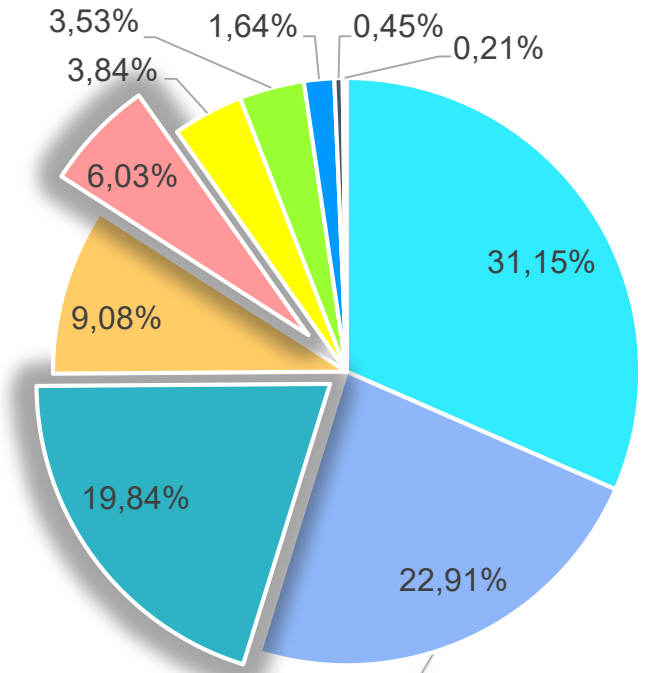
Москва – 2023

ПОЛИТЕХ МЫСЛИТЬ БУДУЩИМ

Актуальность

Статистика частот сетевых атак на май 2022 года, представленная «Лабораторией Касперского»:

- Bruteforce.Generic.Rdp
- Intrusion.Win.MS17-010
- Scan.Generic.PortScan.TCP
- Bruteforce.Generic.Bruteforce.Generic.RDP
- Scan.Generic.PortScan.UDP
- Intrusion.Win.MS17-010
- DoS.Generic.Flood.TCPSYN
- Bruteforce.Generic.Bruteforce.Generic.RDP
- DoS.Win.DNS.Query.exploit
- Intrusion.Generic.CVE-2021-44228.a



ПОЛИТЕХ МЫСЛИТЬ БУДУЩИМ

Анализ методов обнаружения TCP- и UDP-сканирования

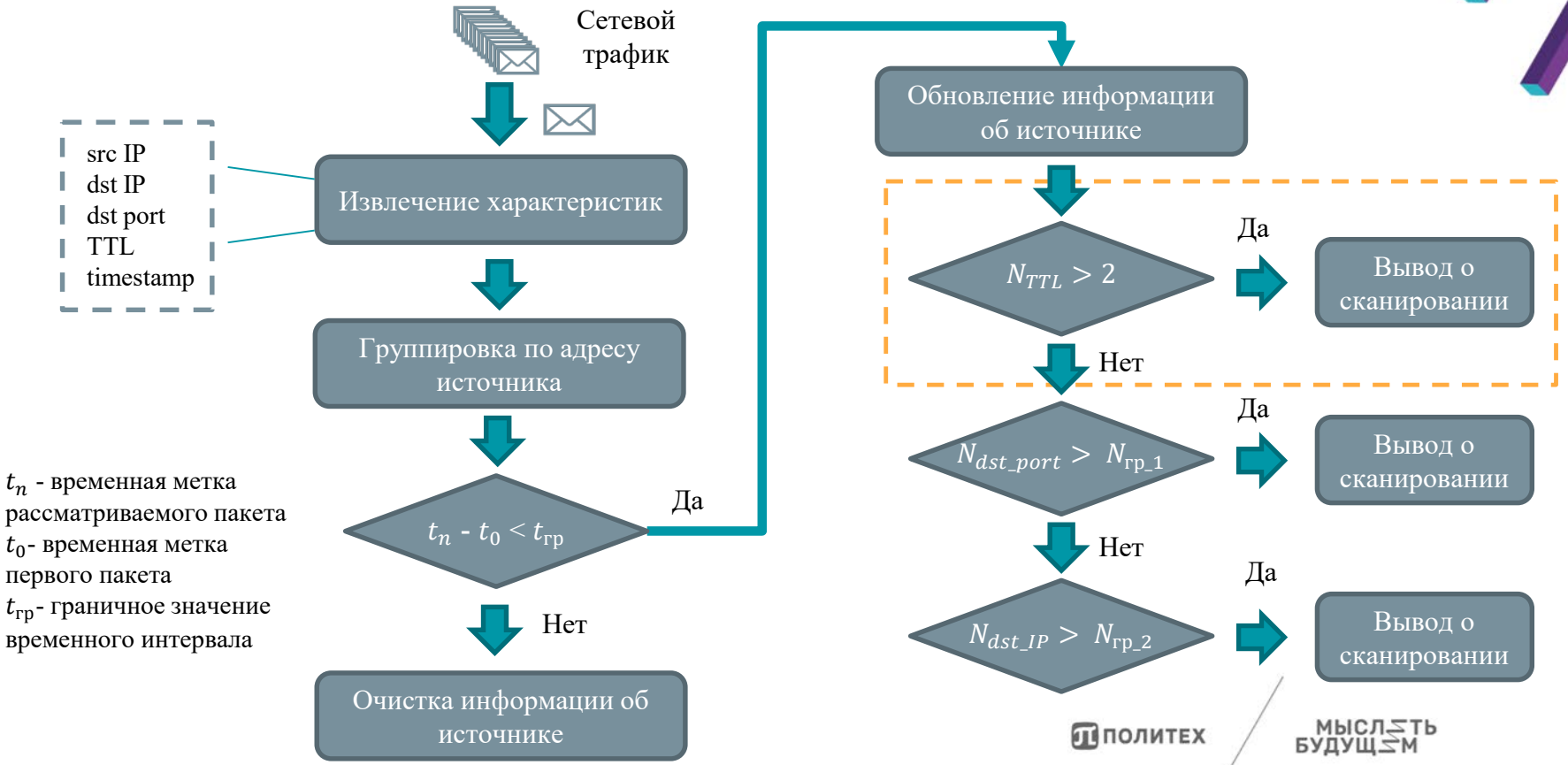
Методы обнаружения	Обнаруживаемые виды сканирования							Количество требуемых пакетов для обнаружения	Ошибки первого рода
	1	2	3	4	5	6	7		
Сигнатурный	–	–	–	+	+	+	–	1	отсутствуют
Поведенческий	+	+	+	+	+	+	+	5-200	присутствуют
Гибридный	+	+	+	+	+	+	+	1-200	присутствуют

1 – TCP Connect 2 – SYN 3 – ACK 4 – NULL 5 – FIN 6 – XMAS 7 – UDP

Способы улучшения гибридного метода:

- Обновление сигнатур
- Сокращение числа требуемых пакетов для выявления SYN- и UDP-сканирования

Модификация поведенческого метода для выявления SYN- и UDP-сканирования



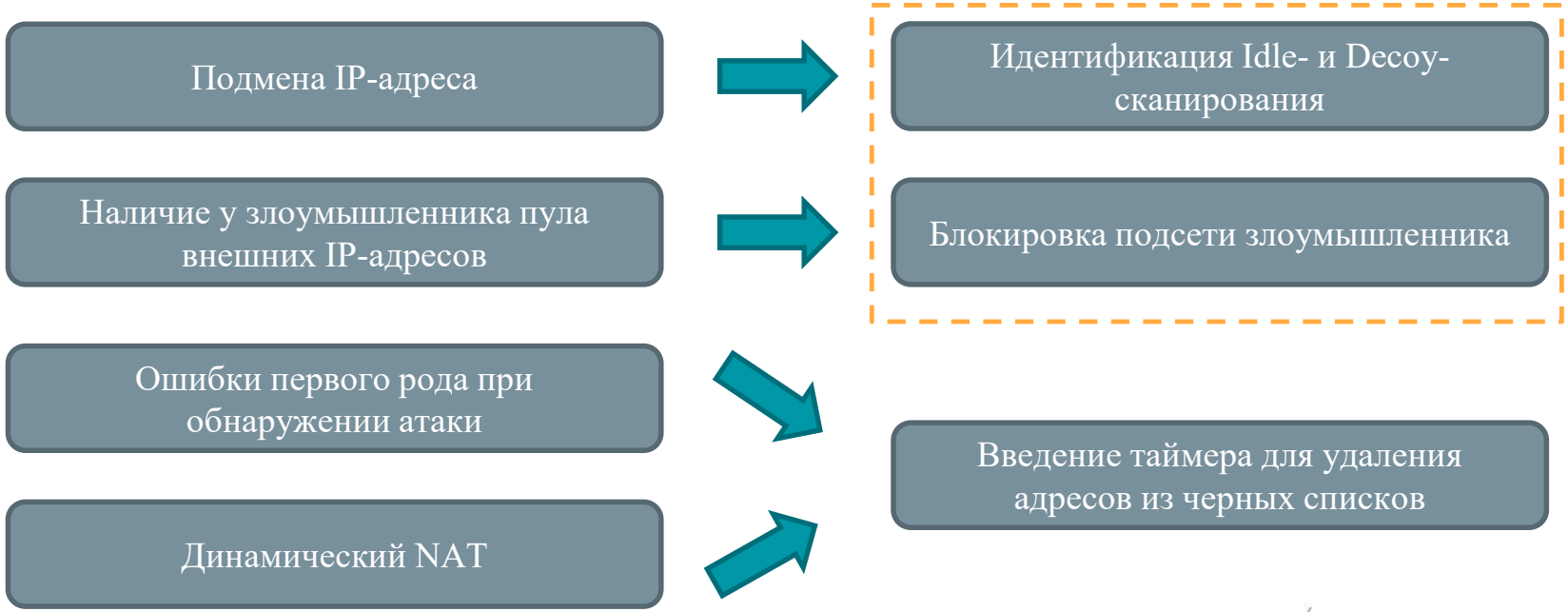
t_n - временная метка рассматриваемого пакета
t_0- временная метка первого пакета
$t_{гр}$- граничное значение временного интервала

ПОЛИТЕХ МЫСЛЯТЬ БУДУЩИМ

Предотвращение дальнейших атак с помощью черных списков

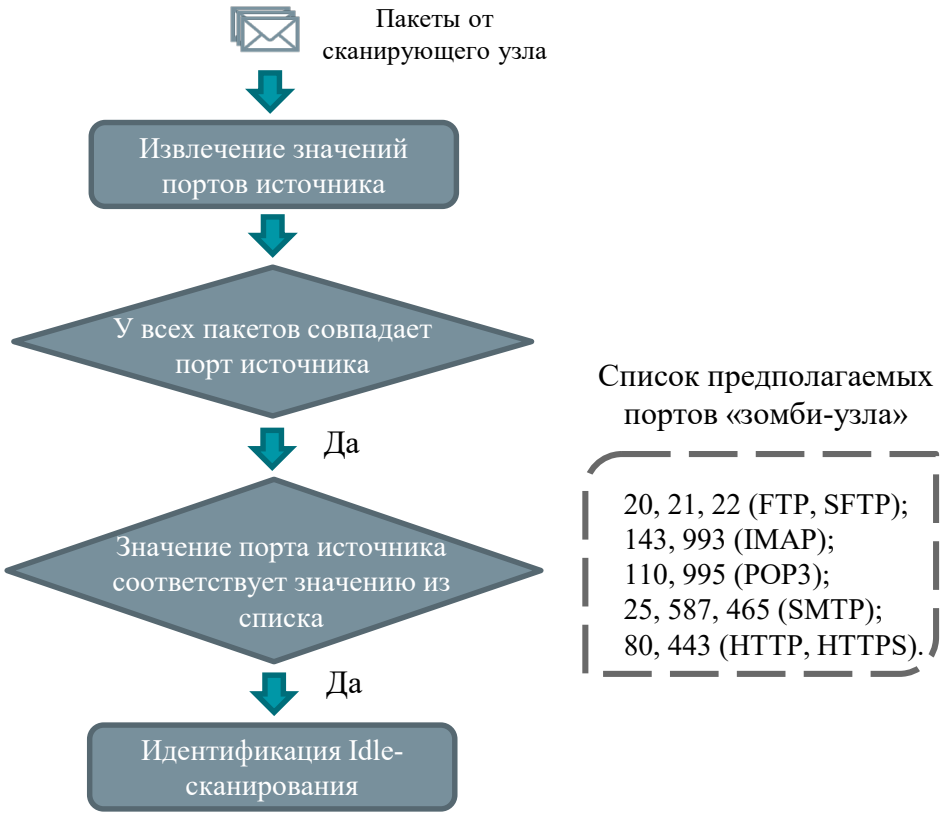
Проблемы при формировании черных списков

Пути их решения

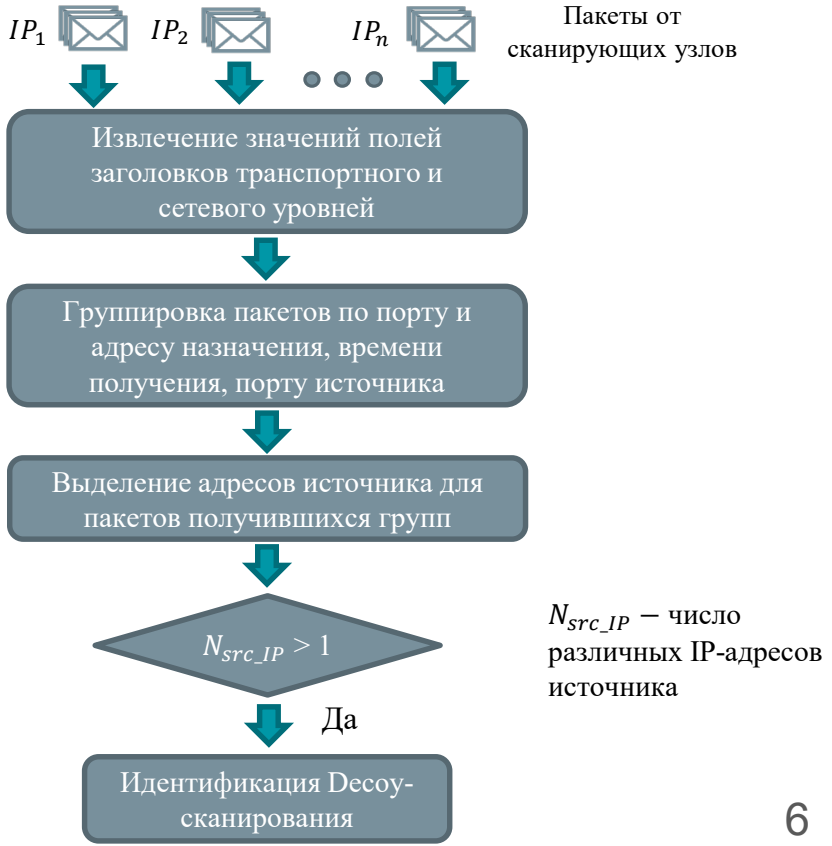


Обнаружение подмены IP-адреса

Идентификация Idle-сканирования



Идентификация Decoy-сканирования



Способ формирования черных списков подсетей

Этапы заполнения черного списка

Дано: IP, список заблокированных подсетей S = [$s_1, \dots, s_n$], граничное значение h.

1. Если S пуст:
   1) вычислить $IP_{\text{подсети}}$ и $IP_{\text{шир.}}$ для IP и маски /30
   2) добавить в S новую подсеть $s = (IP_{\text{подсети}}, IP_{\text{шир.}}, mask)$
   3) выход
2. Если $\exists i: IP \in s_i$, где $i = 1, \dots, n$, то выход
3. Для каждого s_i вычислить $d_i = \begin{cases} d(IP, IP_{\text{подсети}_i}), \text{если } IP < IP_{\text{подсети}_i} \\ d(IP, IP_{\text{шир.}_i}), \text{если } IP > IP_{\text{шир.}_i} \end{cases}$, где $i = 1, \dots, n$
4. Если $d = \min(d_1, \dots, d_n) < h$:
   1) для $s_{index(d)}$ получить $IP_{\text{подсети}}, IP_{\text{шир.}}$
   2) $IP' = \begin{cases} IP_{\text{подсети}}, \text{если } IP > IP_{\text{подсети}} \\ IP_{\text{шир.}}, \text{если } IP < IP_{\text{шир}} \end{cases}$
   3) Вычисление $IP_{\text{подсети}}$", $IP_{\text{шир.}}$", $mask$" для IP и IP'
   4) $s_{index(d)} = (IP_{\text{подсети}}", IP_{\text{шир.}}", mask")$

   Иначе:
   1) вычислить $IP_{\text{подсети}}$ и $IP_{\text{шир.}}$ для IP и маски /30
   2) добавить в S новую подсеть $s = (IP_{\text{подсети}}, IP_{\text{шир.}}, mask)$

Выбор метрики

$$subnet\_mask(IP_1, IP_2) = \sum_{i=\lfloor \log_2(IP_1 \oplus IP_2) \rfloor + 1}^{32} 2^i, \quad IP_1 \neq IP_2$$

Метрика должна учитывать позицию наиболее значимого отличающегося бита

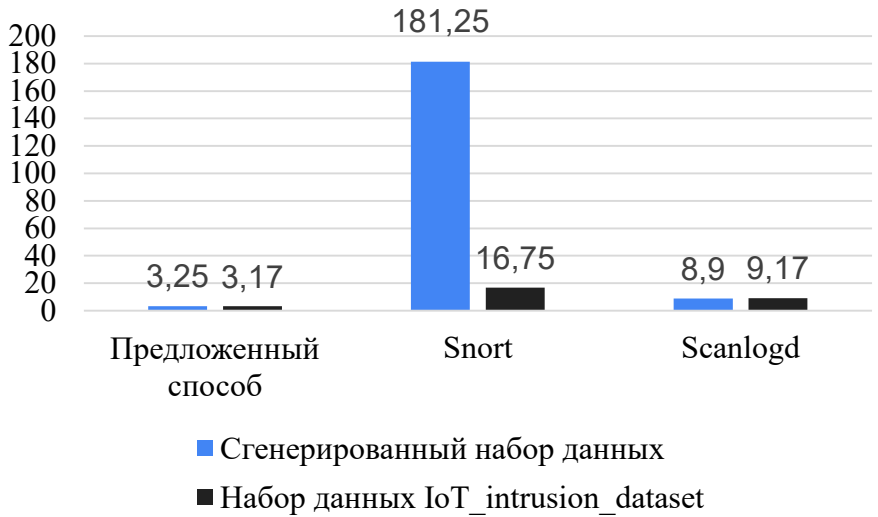
Метрика XOR

$$d(IP_1, IP_2) = \begin{cases} 2^{\lfloor \log_2(IP_1 \oplus IP_2) \rfloor}, IP_1 \neq IP_2, \\ 0, IP_1 = IP_2 \end{cases}$$

Схема разработанного прототипа

Оценка предложенного способа обнаружения сканирования

Среднее количество потребовавшихся пакетов для обнаружения SYN-сканирования



Идентификация Decoy-сканирования

Snort:

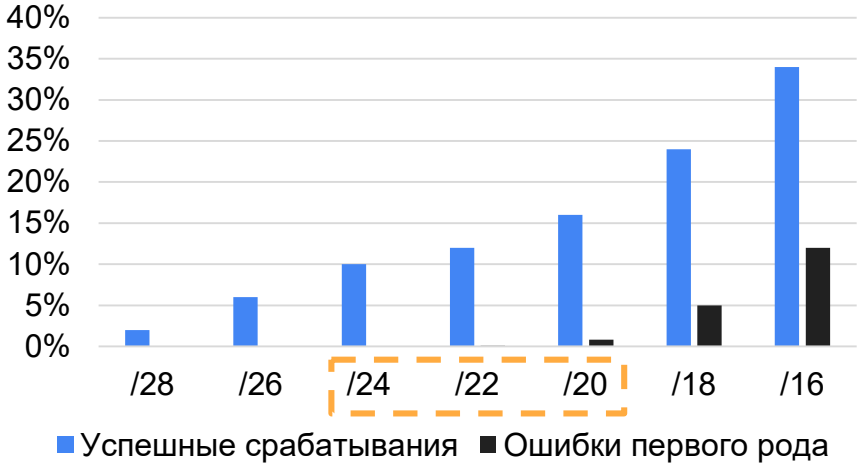
- Идентификация Decoy-сканирования начиная с 25 узлов-приманок
- Определяемый диапазон сканирующих узлов шире, чем он есть на самом деле

Предложенный способ:

- Идентификация Decoy-сканирования начиная с 1 узла-приманки
- Определяет точный список сканирующих узлов

Выбор порогового значения для формирования черных списков подсетей

Оценка пороговых значений



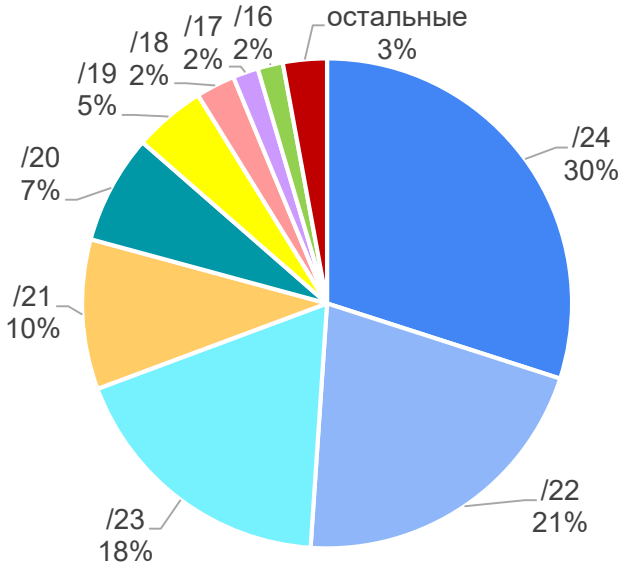
Набор данных

Список вредоносных адресов IPsum

+

Dataset of Malicious and Benign Webpages

Подсети интернет-провайдеров и организаций



Результаты

1. Проанализированы 7 видов сканирования из сети Интернет. Выбран гибридный метод обнаружения сканирования, определены пути его улучшения. Сформулированы проблемы, возникающие при составлении черных списков.

2. Обновлены сигнатуры SYN-сканирования. Предложена модификация поведенческого метода обнаружения сканирования, позволяющая сократить число проанализированных пакетов для выявления SYN- и UDP- сканирования.

3. Разработан способ составления черных списков подсетей для предотвращения дальнейшего распределенного сканирования из сети Интернет, учитывающий наличие пула внешних IP-адресов у злоумышленника, а также подмену IP-адресов.

4. Экспериментально показано, что предложенный способ обнаружения SYN-сканирования позволяет сократить количество проанализированных пакетов в 3 раза по сравнению со Scanlogd, и в 5 раз по сравнению со Snort. Предложенный способ идентификации Decoy-сканирования обладает большей точностью, по сравнению с СОВ Snort. Оценены пороговые значения для предлагаемого способа формирования черных списков подсетей.