УДК 004.3

АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ И ВОЗМОЖНОСТИ АТАК ТИПА «МАЙНИНГ НА ПРОЦЕССОРАХ»

Н.Д. Церкович, 1 курс
Научный руководитель – **В.А. Клаченков**, ассистент
Полесский государственный университет

Основной задачей сети Полесского государственного университета, является предоставление материально-учебной базы, для осуществления образовательного процесса. Хоть локальная сеть и имеет уязвимости к атакам таким как: отказ в обслуживании, apr-атака, mimt-атака, dhcp-spoofing, они не являются актуальными вследствие того, что сеть не имеет ценной информации для злоумышленников. Но как для регионального университета Полесский государственный университет имеет большие мощности в плане компьютерной техники и составляет около 1000 единиц, что в свою очередь, становится актуальным направлением атак злоумышленника с целью нанесению вреда и майнинга криптовалюты. Рассмотрим характеристики процессоров в компьютерной тенники:

Так как системы предназначены для работы и организации учебного процесса, видеокарты отсутствуют. Оперативная память в зависимости от варианта комплектации стоит от 2 до 16 Gb. Блоки питания мощностью от 300 до 500W.

Изучив технические характеристики и комплектацию техники самыми актуальными для злоумышленника будет использование атак майнинга основанных на CPU. Майнинг на процессоре производится аналогично процессу добывания криптовалюты по алгоритму доказательства выполненной работы (PoW).

Самые популярные криптовалюты, которые майнятся на процессорах, используют алгоритм CryptoNote или его модификации, наиболее известными из которых являются Bytecoin, Monero и DarkNote [1].

Технология CryptoNote использует базу транзакций в виде цепочки блоков, похожую на базу Bitcoin. База защищена от модификации методом proof-of-work на основе хэша. Но в CryptoNote время вычислений в большей степени зависит от скорости произвольного доступа к памяти, чем от скорости выполнения простых математических операций.

Таблица – Технические характеристики процессоров и их хешрейт

Наименование	Ryzen 3200G	Core i3-2120	Intel Celeron G3930	Intel® Pentium® G5420 Gold	Core I5-2500	Core I7 - 4770
Ядро	Picasso	Sandy Bridge	Kaby Lake-S	Coffee Lake S	Sandy Bridge	Haswell
Количество ядер	4	2	2	2	4	4
Техпроцесс, нм	12 нм	32 нм	14 нм	14 нм	32 нм	22нм
Разъем	Socket AM4	LGA 1155	LGA 1151	LGA 1151-v2	LGA 1155	LGA 1150
Частота, МГц	3600	3300	2900	3800	3300	3400
Множитель	36	33	29	38	33	34
кэш L1, КБ	4 x (32 + 64)	32+32 x2	64 +64	64 +64	128+128	64x4
кэш L2, КБ	4 x 512	256x2	512	512	1024	1024
кэш L3, КБ	4096	3072	2048	4096	6144	8192
TDP, Вт	65	65	51	54	95	84
Предельная температура, °C	72.6	69.1	70 °C	100°C	72 °C	72°C
Хешрейт(H/s)	5060	396.04	381.89	900	1055.85	4760
Прочие особенности	Разблокирован множитель?	HT,VT,EIST, HD Graphics 2000	Intel HD Graphics 610	Intel HD Graphics 610	Intel HD Graphics 2000	Intel® HD Graphics 4600

Алгоритм включает в себя Keccak (SHA-3) и функцию губки, аналогичный используемому в алгоритме Scrypt буфер размером 2MB, к которому выполняется произвольный доступ на чтение и на запись,64-битные операции умножения, вычисление раунда шифрования AES, дополнительные хэш-функции: BLAKE, Grøstl, JH, Skein.

Анонимность в CryptoNote реализована за счет использования кольцевых подписей (скрывают отправителя) и одноразовых адресов (скрывают получателя) [2].

Для реализации и проведения атак с целью майнинга используются атаки вида криптоджекинг. Криптоджекинг – это схема использования чужих устройств без ведома их владельцев с целью скрытого майнинга криптовалют. Вместо того чтобы строить специализированные компьютерные системы для добычи криптовалют, хакеры прибегают к методам криптоджекинга и похищают вычислительные мощности с устройств своих жертв. Складывая все эти мощности, хакеры могут успешно (а главное – без существенных затрат) конкурировать с крупными игроками на рынке добычи криптовалют. Кража вычислительной мощности замедляет работу компьютера, повышает счета за электроэнергию и сокращает срок эксплуатации устройства.

На сегодняшний день существуют несколько способ проведения атак криптоджекинга.

Программы майнеров на основе вирусов и программ вымогателей. В данном виде майнеров. используются сетевые черви, с помощью которых идет распространение с одного зараженного компьютера на другие машины, подключенные к той же сети. Особенность связки с программами вымогателями является то, что при нахождении майнера и его удалении, запускается программа вымогатель, которая блокирует работу системы.

Программы майнеры на основе фишинга. Данный вид основан на том, что пользователь откроет вредоносную ссылку или вложение в электронной почте. Остается весьма популярным и эффективным направлением атак.

Браузерный майнинг. Данный вид основан на внедрении JavaScript-файла в структуру сайта, который использует мощность компьютера посетителя для добычи цифровой валюты.

Рассмотрим наиболее популярные криптоджекеры, которые могут быть использованы на локально-вычеслительную сеть Полесского университета и устройства, находящихся в ней:

Smominru — ботнет, который специализируется на добыче криптовалюты Monero, чему способствовала интеллектуальная структура сети с постоянным самовосстановлением. Smominru работал на основе эксплойта EternalBlue, украденного у АНБ, который также использовался для распространения мировой эпидемии программы-вымогателя WannaCry. EternalBlue (CVE-2017-0144) - название эксплоита, который использует уязвимость в Windows-реализации протокола SMB и использует функцию Windows с именем srv!SrvOS2FeaListSizeToNt.

Майнинговый код Coinhive изначально разрабатывался (и до сих пор используется) как законное средство монетизации веб-сайтов, но к настоящему времени стал крупнейшей в мире угрозой криптоджекинга. Интересно, что компания, ответственная за Coinhive, получает 30 процентов со всех операций майнинга, в том числе со взломанных экземпляров.

MassMiner – любопытный пример, который необычен тем, что использует множество эксплойтов разных уязвимостей в одном пакете. Эксплуатация неисправленных уязвимостей в Oracle WebLogic, Windows SMB и Apache Struts принесла создателям MassMiner почти 200 000 долларов в криптовалюте Monero.

Prowli – это сетевой червь для подбора паролей методом полного перебора, чтобы ускорить распространение майнера криптовалюты Monero. В некоторых случаях ботнет также устанавливает бэкдоры на зараженные системы.

WinstarNssmMinerB данный криптоджекер бездействует, если на целевой машине обнаружено эффективное антивирусное ПО, и активируется только на системах со слабой защитой. Кроме того, при попытке удалить WinstarNssmMiner зараженная система выходит из строя.

Список использованных источников

1. CryptoNote [Электронный ресурс] Гнездо строителя дизайн и ремонт интерьеров // Режим доступа: https://gnezdoparanoika.ru/stati/24179-cryptonote.html - Дата доступа: 20.03.2023.

2. Monero: как достигается анонимность [Электронный ресурс] // Режим доступа: https://tgraph.io/Monero-kak-dostigaetsya-anonimnost-05-09-2 - Дата доступа: 20.03.2023.