НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

РІЗКЕ ЗРОСТАННЯ КІБЕРАТАК НА УКРАЇНСЬКІ УСТАНОВИ З ВИКОРИСТАННЯМ SMOKELOADER

РЕЗЮМЕ

З травня цього року російські кіберзлочинці різко активізували використання шкідливого програмного забезпечення Smokeloader проти українських фінансових та урядових організацій. Smokeloader – це складний і багатофункціональний зразок шкідливого програмного забезпечення, який обирають зловмисники для проникнення і компрометації критично важливих інституцій.

У цьому звіті представлено поглиблений аналіз еволюції тактик і стратегій, що застосовуються цими кіберзлочинцями, висвітлюючи їхні мотиви, методи та потенційний вплив.

Якщо раніше українські організації здебільшого атакували спонсоровані державою російські APT угруповання, то зараз зростання кількості атак з використанням Smokeloader говорить про збільшення загрози від російських кіберзлочинних угруповань.

ТУМАН SMOKELOADER

Шкідливе програмне забезпечення Smokeloader як потужний інструмент з’явилось у даркнеті ще у 2011 році. Останнім часом зловмисники використовують його для атак на українські організації, адже він має широкий спектр функцій, що робить його цінним активом для зловмисників. Smokeloader непомітно проникає в систему, викрадає дані та надає віддалений доступ до скомпрометованої системи. Ціна цього шкідливого програмного забезпечення варіюється **від 400 доларів США за базовий бот до 1650 доларів США за повний пакет** з усіма доступними плагінами та функціями.

3 травня 2023 року російські кіберзлочинці використовують Smokeloader як основний інструмент для організації низки атак на українські об'єкти. Щомісяця вони запускають великі хвилі фішингових атак, маскуючи шкідливі електронні листи під фінансову тематику.

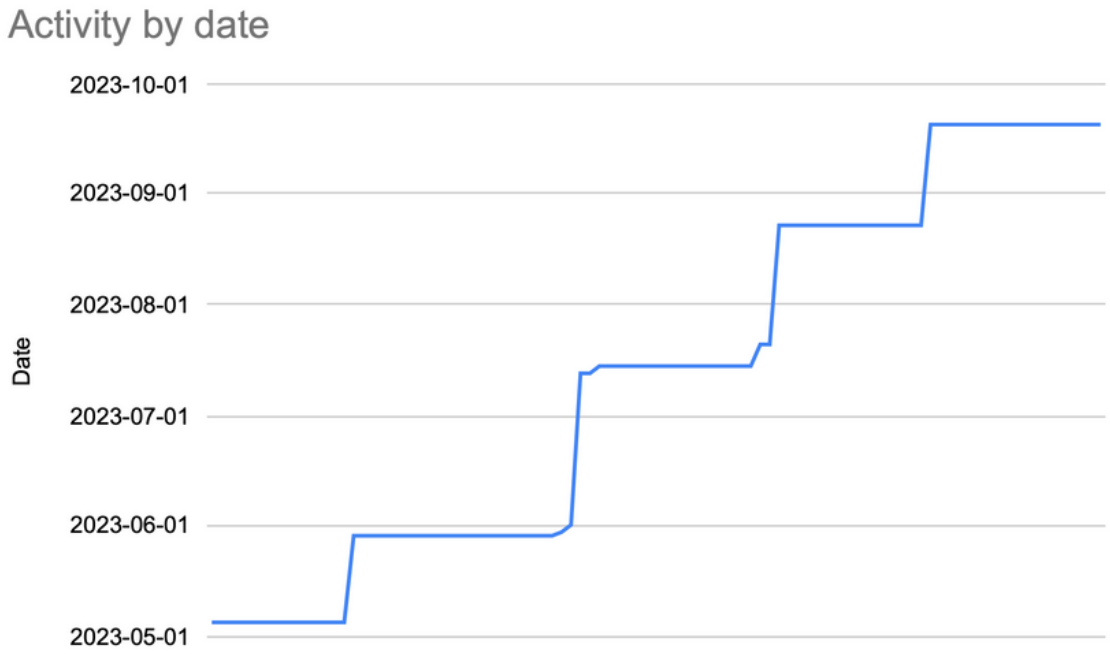

Рис.1. Хронологія діяльності кіберзлочинців

Детальний аналіз їхньої мережевої інфраструктури виявив велику кількість російських реєстраторів доменів, таких як REGRU, REGTIME і RU-CENTER. Це говорить про те, що кіберзлочинці мають зв'язки з росією.

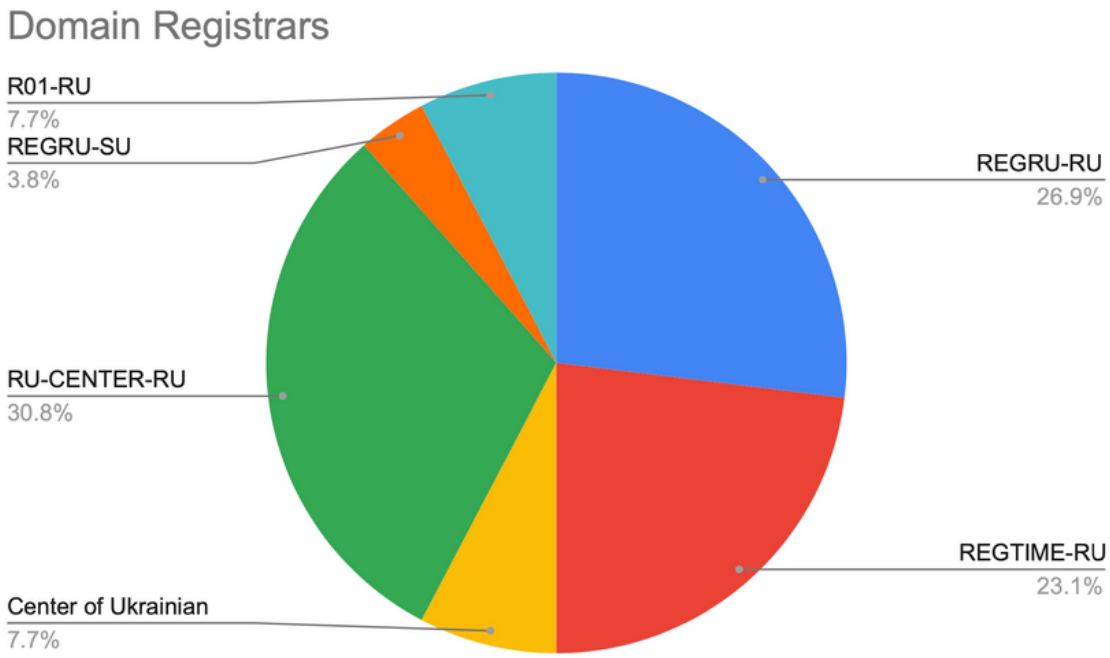

Рис. 2. Розподіл реєстраторів доменів, якими користуються кіберзлочинці

ОМАНЛИВА ТАКТИКА

Нещодавні кампанії Smokeloader продемонстрували витонченість у своїх тактиках і методах, з акцентом на фінансовій тематиці. Зловмисні операції починаються з ретельно розроблених фішингових електронних листів, призначених для заманювання та обману жертв. Фінансові теми домінують у змісті, створюючи відчуття терміновості та актуальності для одержувачів.

Рис. 3. Фішинговий електронний лист зі Smokeloader та фінансовою тематикою

Однак основний пейлоад приховується у вкладенні – зазвичай в архівному файлі, інкапсульованому кілька разів. Всередині цього цифрового лабіринту знаходяться файли на фінансову тематику, які слугують приманкою. Жертви проходить через ці рівні шифрування, поки не досягнуть основного пейлоаду – Smokeloader.

Слід зазначити, що ці кампанії мають характерні ознаки, які вказують на причетність російських кіберзлочинців. Орфографічні помилки та розбіжності в назвах українських документів у шкідливих вкладеннях свідчать про недостатнє знання мови.

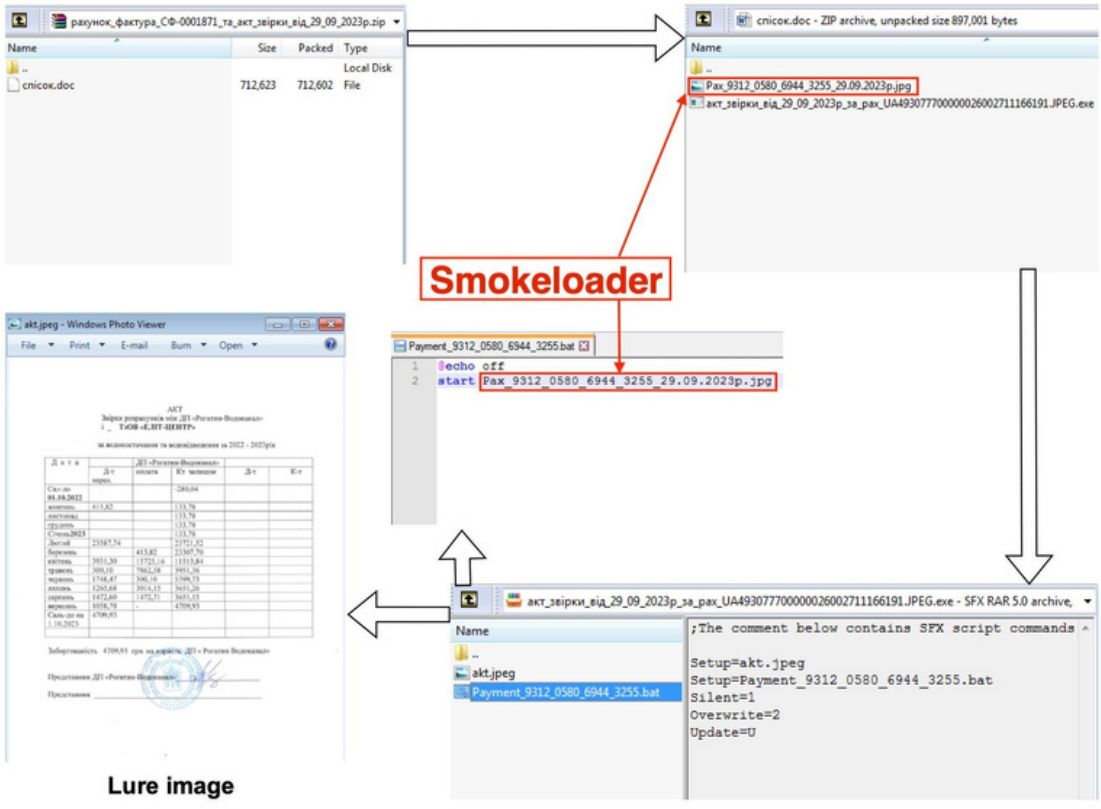

Рис.4 Приклад ланцюга зараження Smokeloader

Під час запуску основного пейлоаду шкідливого програмного забезпечення жертви отримують легітимні фінансові документи, щоб зменшити підозри та надати їм більш правдивого вигляду. Ці легітимні документи були викрадені з раніше скомпрометованих організацій.

Під час розгортання шкідливе програмне забезпечення Smokeloader виконує складні та приховані операції та починає встановлювати зв'язок із заздалегідь визначеним списком командно-контрольних серверів (C2). Цей список закодований у конфігурації шкідливого програмного забезпечення:

{"Version": 2022, "C2 list": ["http://super777bomba.ru/", "http://dublebomber.ru/", "http://yavasponimayu.ru/", "http://nomnetozhedenyuzhkanuzhna.ru/", "http://restmantra.by/", "http://prostosmeritesya.ru/", "http://iloveua.ir/", "http://kozachok777.ru/", "http://ipoluchayteudovolstvie.ru/", "http://propertyminsk.by/", "http://tvoyaradostetoya.ru/", "http://propertyiran.ir/", "http://moyabelorussiya.by/"]}

Підступність Smokeloader, також, полягає у його вибірковій комунікації. Багато з цих доменів залишаються навмисно недоступними, діючи як приманки, щоб відвернути увагу та ускладнити зусилля з виявлення.

БАГАТОГРАННА ФУНКЦІОНАЛЬНІСТЬ

Smokeloader, який давно присутній на даркнет форумах, починаючи з 2011 року, є багатофункціональним і прихованим шкідливим програмним забезпеченням. Він налічує величезний набір функцій для того, щоб запобігти його аналізу та виявленню. Методи антианалізу цього шкідливого програмного забезпечення включає низку функцій для захисту Smokeloader від спроб здійснити debugging, hooking та проаналізувати шкідливе програмне забезпечення у віртуальному середовищі експертами з кібербезпеки.

Крім можливостей антианалізу, Smokeloader може отримувати важливу системну інформацію, таку як деталі операційної системи та географічні дані, пропонуючи зловмисникам цінну інформацію про середовище зараженої системи.

Здравствуйте, уважаемые форумчане, предлагаю Вам собственную разработку:

Smoke Bot - это модульный бот, в основе которого используется функционал резидентного лоадера

Преимущества:
- наличие модулей-плагинов, которые расширяют функционал бота, при этом не влияют на размер бота (не нуждаются в криптовании)
- подробная статистика по версиям ОС (разрядность, привилегии), странам и онлайну
- подробная статистика по заданиям, загрузки/запуски, ограничение на количество и т.п.
- задания для бота на загрузку EXE или DLL (LoadLibrary, regsvr32, запуск из памяти без сохранения на диск)
- гео-таргетинг (выборочные загрузки только для конкретных стран или блокировка для определенных стран)
- персональные задания для каждого бота, возможность бана или удаления бота
- поддержка HTTPS, скачивание файлов заданий с админки или другого URL
- незаметная установка в системе, защита собственных файлов
- возможность обновления бота и резервные адреса для отстука
- возможность использования префиксов (ID) для exe (более точная статистика и разделение заданий)
- исключение повторного запуска на машине с уже работающим ботом (в рамках одной лицензии)
- "гостевой" доступ к статистике заданий
- обход проактивных механизмов AB (инжектирование в доверенный процесс)
- повышение привилегий Low->High (runas + cmd)
- антиотладка, антиэмуляция, детектирование "песочниц" и виртуальных машин
- легок в криптовании (не содержит в себе дополнительных DLL, оверлеев, TLS, всего одна секция кода)
- работа в Windows 7-10 x32/x64
- небольшой размер бота ~35 Кб

Рис. 5. Тема на даркнет форумі з продажу шкідливого програмного забезпечення Smokeloader

Для подальшого розширення своїх можливостей Smokeloader використовує модульну конструкцію. Ці модулі дозволяють шкідливому програмному забезпеченню адаптуватися та розвиватися, пристосовуючи свої шкідливі операції до конкретних цілей зловмисників.

Module	Features
STEALER	Збирає облікові дані та файли cookie з різних програм (браузерів, поштових клієнтів, FTP).
FORM GRABBER	Перехоплює POST-запити веббраузера до того, як вони пройдуть через шифрування.
PASS SNIFFER	Перехоплює облікові дані найпоширеніших програм і протоколів (FTP, POP3, IMAP, SMTP).
FAKE DNS	DNS Spoofing. Повертає неправильну IP-адресу для доменного імені за певним правилом.
FILE SEARCH	Виконує пошук файлів і надсилає їх зловмисникам.
PROCMON	Моніторинг і взаємодія з процесами.
DDOS	Виконує DDoS-атаки.
KEYLOGGER	Перехоплює натискання клавіш.
REMOTE PC	Шпигує та керує віддаленим комп'ютером з функціями файлового менеджера.
EMAIL GRABBER	Збирає адреси електронної пошти.

У деяких останніх випадках зловмисникам вдалося скомпрометувати процес грошових переказів, фактично перехопивши контроль над потоком транзакцій. Замість того, щоб кошти потрапляли за призначенням, зловмисники замінювали реквізити рахунків на свої власні. Це призвело до перенаправлення коштів організації на рахунки зловмисників. Такі випадки підкреслюють еволюцію тактики кіберзлочинців, які тепер не лише намагаються проникнути в мережі організацій, але й маніпулюють критично важливими фінансовими процесами для викрадення активів.

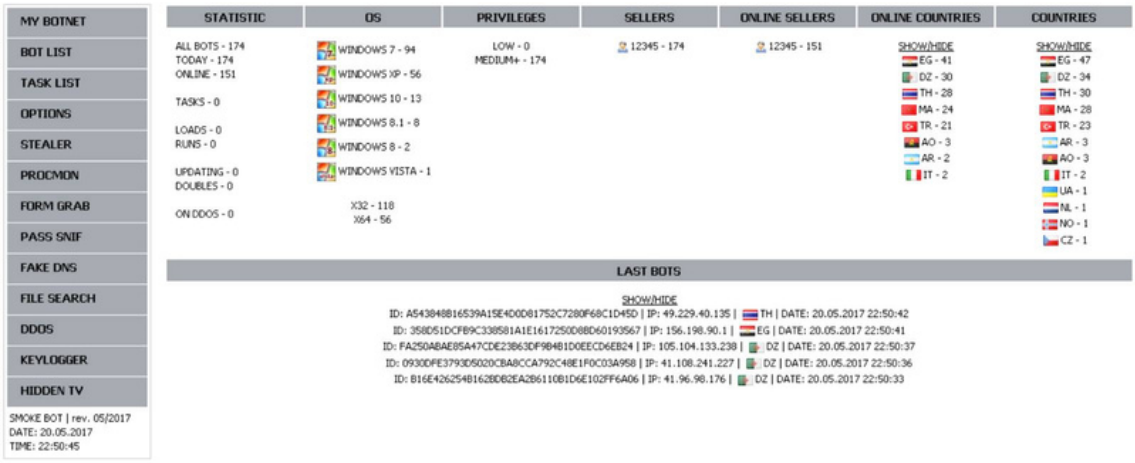

Рис.6 Адмін панель Smokeloader

ВИСНОВОК

Нещодавнє різке зростання атак Smokeloader, організованих російськими кіберзлочинцями проти українських організацій, підкреслює постійно зростаючий і диверсифікований характер кіберзагроз. Ці зловмисники не лише активізували свої операції, але й продемонстрували неабияку адаптивність у своїй тактиці, націлившись на фінансові операції. Таким чином, ландшафт загроз в Україні перетворився на багатогранну арену, де поряд зі спонсорованими державою російськими APT угрупованнями в боротьбу вступають фінансово вмотивовані кіберзлочинці.

У світлі цих подій організаціям в Україні рекомендується зберігати пильність і діяти на випередження в питаннях кібербезпеки. Необхідно інвестувати в навчання персоналу, щоб підвищити обізнаність щодо фішингових електронних листів на фінансову тематику, які є основною точкою входу для атак Smokeloader. Захист кінцевих точок, налаштування систем виявлення вторгнень (IDS) для виявлення загроз у режимі реального часу, а також запровадження суворих обмежень на виконання скриптів і виконуваних файлів з архівів є важливими заходами для зміцнення захисту.

Крім того, безперервний збір розвідданих про загрози та обмін ними для виявлення ознак компрометації через такі платформи, як MISP (Malware Information Sharing Platform), є критично важливими. Постійне інформування про нові загрози і тактики, які застосовують вороги, має першорядне значення для побудови стійкого захисту від загрози Smokeloader і пов'язаних з нею багатогранних викликів. У цьому динамічному середовищі проактивні та спільні зусилля з кібербезпеки є ключем до захисту цифрових кордонів України.

ІНДИКАТОРИ КОМПРОМЕТАЦІЇ ОСТАННЬОЇ КАМПАНІЇ

Type	Value
domain	dublebomber.ru
domain	yavasponimayu.ru
domain	nomnetozhedenyuzhkanuzhna.ru
domain	prostosmeritesya.ru
domain	ipoluchayteudovolstvie.ru
domain	super777bomba.ru
domain	specnaznachenie.ru
domain	zakrylki809.ru
domain	propertyminsk.by
domain	iloveua.ir
domain	moyabelorussiya.by
domain	tvoyaradostetoya.ru
domain	zasadacafe.by
domain	restmantra.by
domain	kozachok777.ru
domain	propertyiran.ir
domain	sakentoshi.ru
domain	popuasyfromua.ru
domain	diplombar.by
domain	ukr-net-download-files-php-name.ru
ip-address	85.143.172.45
sha256	fdf8a89e8c90ed0653780acc77c180185b8971e62d2a02dca2abcfc456d05bd96
sha256	493f708129bf25ff4bb734c179d336f223d9d21ea53b7e5e52f9535a72415bfd
sha256	6999f5f3c6824f27b5a1fb436c59d369f6f1ec08365d48cd1c8d21d1058eaafc
sha256	9a528b2b31d9d59018878fdf3b9d8db235df606500c67a4b8be3075701b014fc
sha256	d895f40a994cb90416881b88fadd2de5af165eec1cd41b0ddd08fa1d6b3262bb
sha256	2c44c9b445d2efc2f46e463d933da2ffc1d3ba6718bd67d3957c3f916b7c79fe
sha256	41b74077e7707dfce2752668a3201e3bc596ade5594535c266e3249c2e697cb2
sha256	40c9bc7186f21b6e2a7da28632e70d9b9bce01cc63c692d4383ac03e13e45533
sha256	ac1aedd7d08d3e92ded28d07944d8a8039650a36dec8b4a5d7b675ce2c5512c4
sha256	ebbf474d69519b7ded60c1dab807dab492c33d9caf76e6495c2ee92be573011e
sha256	739e735aa73cfdbfc08c696e0426434aa78139110b416313d2a39d93915ee318
sha256	0f93344347469ebef7b0d6768f6f50928b8e6df7bc84a4293b7c4a7bb5b98072
sha256	7d7262ab5298abd0e91b6831e37ef0156ded4fdceeaf8f8841c9a80d31f33f8e
sha256	b24c99ca816f7ac8ca87a352ed4f44be9d8a21519dd1f408739da958b580be0c
sha256	cfc44f1399e3d28e55c32bcc73539358e5ac88c0d6a19188a52b161b506bea91
sha256	a8a3130c779904e23b50d69b4e73a714b345e296feebb9f64a732d5c73e7973b
sha256	0a83fcb0b40f35bf6020ad35cedf56b72a6f650a46dc781b2ea1c9647e0f76cc
filename	1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js
filename	2.Акт_звірки_від_03.10.2023_Рах_UA493077700000026002711166194.XLS.js
filename	3.Витяг_з_реєстру_від_03.10.2023_Рах_UA493077700000026002711166194.XLS.js
filename	mstsc.exe
filename	Список_документів_для_ознакомлення.pdf
filename	Список_документів_для_ознайомлення.zip

Type	Value
filename	Список_документів_для_ознайомлення.zip
filename	лист.pdf
filename	2.Акт_звірки_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.js
filename	mstsc.exe
filename	лист.zip
filename	ЗАЯВА.xlsx
filename	Рахунок_до_оплати_389.zip
filename	Рахунок_до_оплати_389.pdf
filename	Рахунок_до_оплати_389.exe
filename	pax_389.exe
filename	Рахунок_до_оплати_389.zip