# Целевые атаки на промышленные компании с использованием шифровальщика Snake

**Дата публикации: 17.06.2020**

**Обновлено: 07.07.2020**

По данным Kaspersky ICS CERT в настоящее время продолжаются направленные атаки на промышленные компании с использованием шифровальщика Snake.

8 июня 2020 стало известно о неполадках в компьютерной сети японского мото- и автопроизводителя Honda в Европе и Японии. В частности, сообщалось о технических трудностях в работе службы поддержки клиентов Honda и финансовых служб компании. ИБ-эксперты полагают, что, вероятнее всего, один из серверов компании был заражен вымогательским ПО Snake (EKANS).

Некоторые исследователи обнаружили на VirusTotal образец вредоносной программы Snake, который проверяет доменное имя компании Honda «mds.honda.com» (вероятно, использующееся во внутренней сети компании). Если доменное имя не удается разрешить (определить IP-адрес), работа вымогателя завершается без шифрования каких-либо файлов. По мнению исследователей, это может указывать на целенаправленные действия злоумышленников.

Эксперты Kaspersky ICS CERT, используя данные собственной телеметрии, обнаружили также и другие образцы, сходные с тем, который был загружен на VirusTotal. Согласно результатам нашего исследования:

1. Вредоносное ПО запускалось с использованием файла «nmon.bat», обнаруженного продуктами «Лаборатории Касперского» в каталогах скриптов доменных политик.
2. Все выявленные образцы Snake отличаются лишь зашитым в код доменным именем и IP-адресом.
3. Зашитый в код вредоносного ПО IP-адрес используется для сравнения с IP-адресом доменного имени, если его удалось разрешить.
4. Шифрование данных производится только в случае совпадения IP-адреса в коде вредоносной программы и IP-адреса, который вредоносное ПО получает в случае успешного разрешения доменного имени, также зашитого в код вредоносной программы.
5. Комбинация IP-адреса и доменного имени, зашитых в код вредоносной программы, уникальна для каждой обнаруженной нами атаки и относится, по всей видимости, к внутренней сети той организации, на которую была направлена конкретная атака.
6. В некоторых случаях доменное имя могло быть получено из публичных источников (DNS), а информация о его связи с IP-адресом, по всей видимости, хранится на внутреннем DNS и доступна только при обращении к DNS из внутренней сети организации-жертвы.
7. Помимо зашитых в код доменного имени и IP-адреса атакуемой организации новые образцы Snake отличаются от тех, что были обнаружены в декабре 2019 года, дополненным списком расширений (типов) файлов, которые вредоносное ПО должно шифровать. В новых образцах были добавлены расширения файлов

виртуальных дисков, Microsoft Access, исходных кодов C/C#/ASP/JSP/PHP/JS, а также соответствующих файлов проектов/решений и другие.

Результаты нашего исследования явно указывают на то, что злоумышленники проводят многоступенчатые хакерские атаки, при этом каждая атака направлена на конкретную организацию. Шифрование данных при помощи Snake – конечный этап этих атак.

Каждый образец Snake был, по всей видимости, скомпилирован после того, как злоумышленникам стали известны доменное имя и связанный с ним IP-адрес во внутренний сети компании. IP-адрес и доменное имя хранятся в изученных образцах вредоносного ПО в виде строк, что с учётом их переменной длины исключает возможность легко изменить (пропатчить) исполняемый файл после его компиляции.

Очевидно, что проверка соответствия доменного имени и IP-адреса является техникой, позволяющей предотвратить работу вредоносного ПО за пределами локальной сети, для которой оно предназначено.

Вероятнее всего для распространения шифровальщика внутри локальной сети злоумышленники использовали доменные политики, т.е. имели доступ к учётной записи доменного администратора, скомпрометированной на предыдущих этапах атаки.

Известно, что помимо Honda в числе жертв оказались также энергетические компании Enel Group. По данным Kaspersky ICS CERT, целью атак стали также немецкая компания - поставщик изделий для автомобилестроительных компаний и промышленного производства и немецкая компания, занимающаяся производством медицинского оборудования и расходных материалов.  По всей видимости, атаке подверглись также и другие автомобилестроительные и производственные компании – схожие экземпляры Snake были обнаружены на компьютерах в Китае, Японии и в Европе. По нашим оценкам атакой могли быть затронуты не только IT-системы жертв. Так, в одном случае вредоносное ПО было обнаружено и заблокировано на сервере видеонаблюдения одной из атакованных организаций в Китае.

Все обнаруженные образцы вредоносного ПО проактивно блокировались продуктами «Лаборатории Касперского» при помощи поведенческой сигнатуры Trojan-Ransom.Win32.Snake.a, созданной на основе первого образца Snake, появившегося в декабре 2019 года.

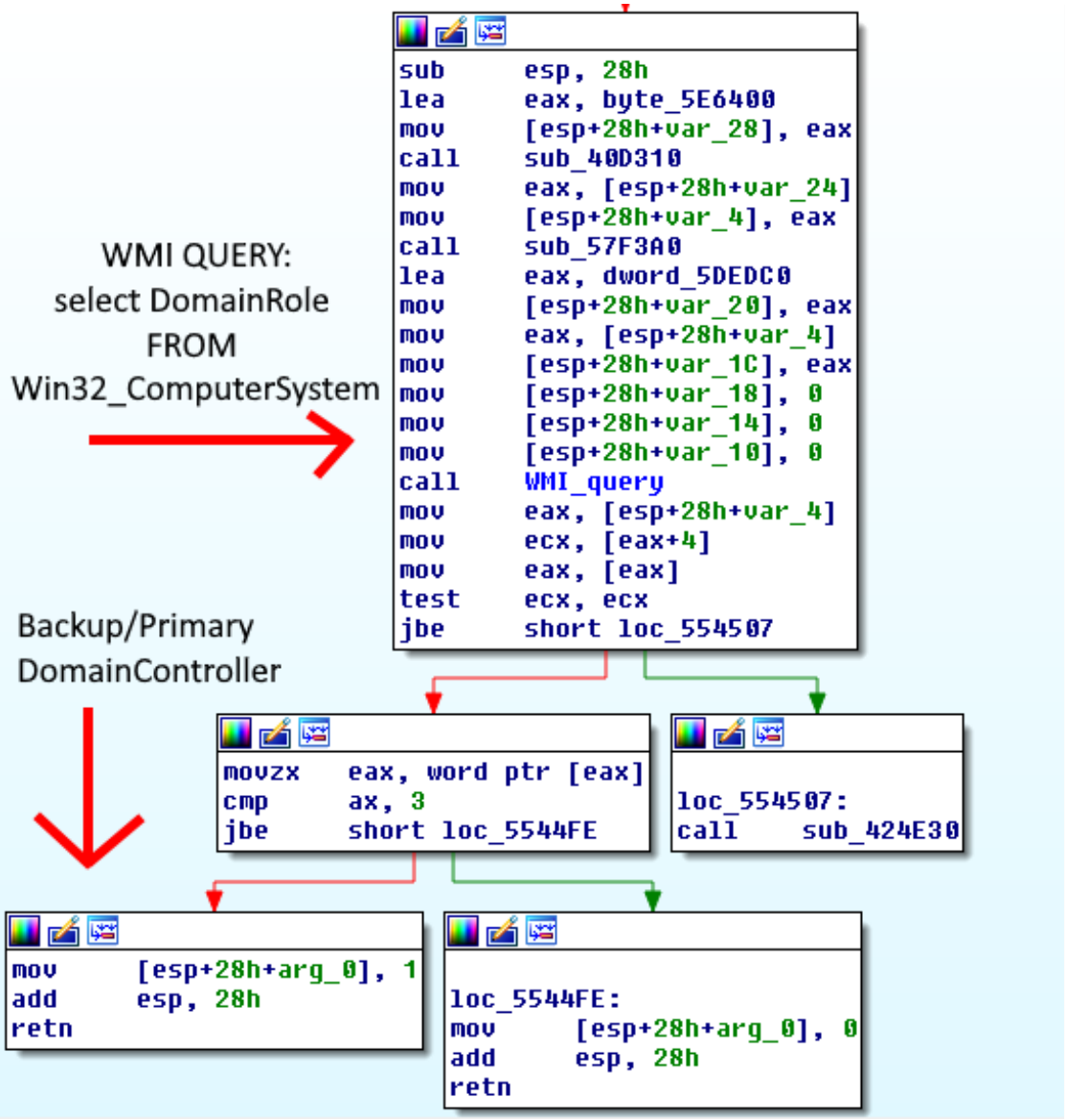
Напомним, что одной из важных особенностей Snake является нацеленность, в том числе, на системы автоматизации промышленных предприятий, а именно – способность шифрования файлов, относящихся к АСУ от General Electric. Об этом свидетельствует попытка вредоносного ПО принудительно завершать процессы ПО General Electric перед началом шифрования.

Подобные атаки продолжаются и в настоящее время. Если вы столкнулись с такой атакой, вы можете сообщить нам об этом, воспользовавшись специальной формой на нашем веб-сайте.

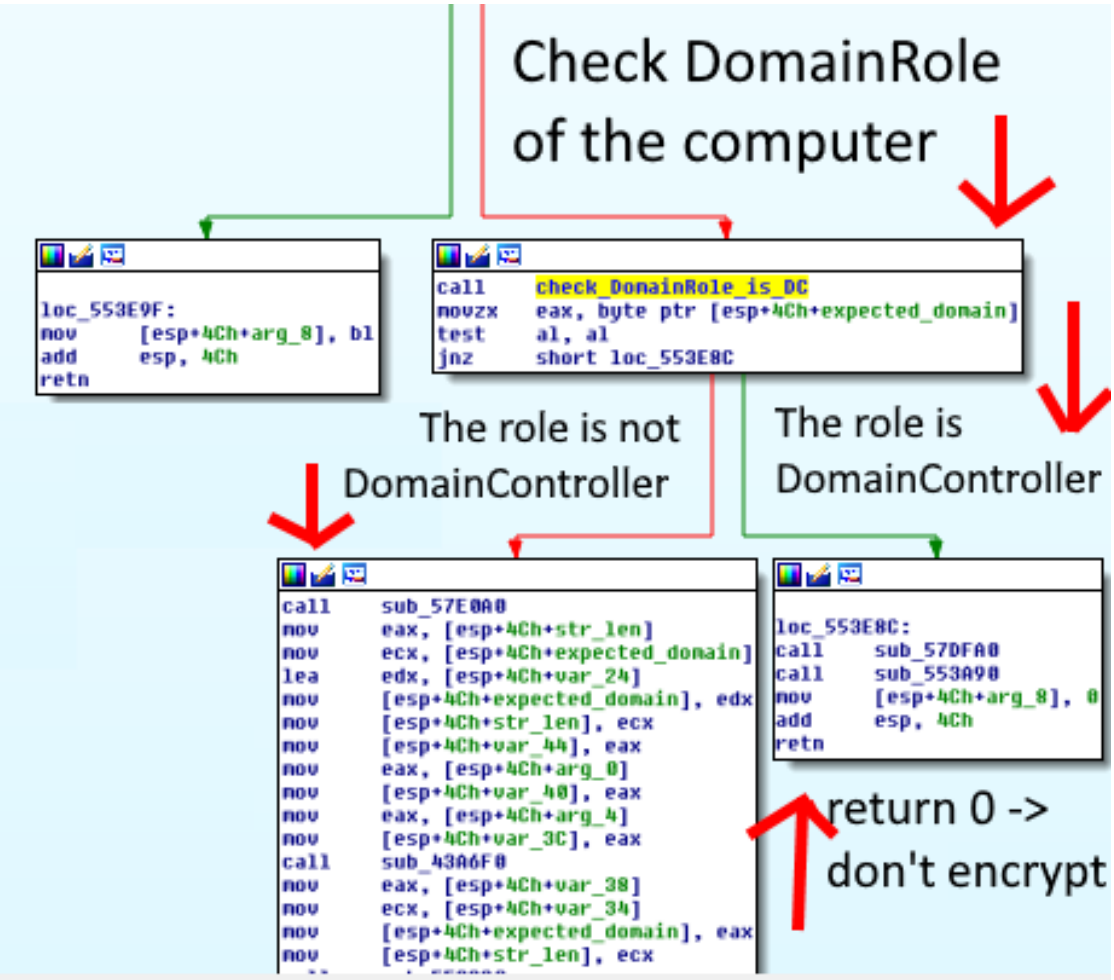
# Обновление 07.07.2020

Наше предположение о том, что для распространения шифровальщика внутри локальной сети злоумышленники использовали контроллер домена атакуемой компании, подтверждает еще один интересный факт.

Вредоносное ПО проверяет доменную роль компьютера, на котором оно запущено. Если компьютер имеет роль контроллера домена (DomainController), функция проверки возвращает «1».




Если функция проверки доменной роли атакованного компьютера возвращает «1» (т.е. компьютер имеет роль основного или второстепенного контроллера домена), то вызывающая её функция возвращает «0», что приводит к завершению работы вредоносной программы без выполнения шифрования. В вызывающей функции проверяется также соответствие IP адреса домена и IP адреса, зашитого в код.




Таким образом, если, как мы считаем, злоумышленники использовали контроллер домена для распространения вредоносного ПО внутри локальной сети жертвы, то описанная логика исключения контроллера домена очевидно была им необходима – контроллер домена нужен им работающим и незашифрованным.

# Рекомендации

Для выявления следов атаки и предотвращения возможного ущерба Kaspersky ICS CERT рекомендует:

- Использовать предоставленные индикаторы компрометации для выявления заражения на рабочих станциях и серверах под управлением Windows;
- Проверить активные доменные политики и скрипты на предмет наличия вредоносного кода;
- Проверить активные задачи в планировщике заданий Windows на рабочих станциях и серверах на предмет наличия вредоносного кода;
- Сменить пароли для учётных записей, входящих в группу доменных администраторов.

# Индикаторы компрометации

## MD5

- ED3C05BDE9F0EA0F1321355B03AC42D0
- 7DDB09DB3FB9B01FA931C2A1A41E13E1
- C547141B8A690EEE313C0F6CE6B5CCA6
- 47EBE9F8F5F73F07D456EC12BB49C75D
- D659325EA3491708820A2BEFFE9362B8
- C7C39967E16500C37638AB24F1BB3FF9
- F58A00D132205045F8AA4C765239301F
- D1277A10494B5D2D5B21B2488C650D3A
- 1E296139AF94AFC2F6002969E8EA750E
- E52927F8E4A22B4D9FD463637A8696EE
- 6DDD81BE14DFC8354AEB63220CFE112E
- DC68AE3CC7BDB1EC80C72FC9F0E93255

## Имена файлов

- nmon.exe
- nmon.bat
- KB3020369.exe
- KB[7 random numbers].exe

## Папки, в которых могут располагаться вредоносные объекты

- %WinTemp%
- \sysvol\[domain name]\scripts\

**Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT)** — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com