IstroSec

Arkusz danych

Analiza złośliwego oprogramowania

Cyberataki są najczęściej przeprowadzane poprzez złośliwe oprogramowanie, tzw. malware. Bardzo często wykorzystuje się także ransomware i inne cyberataki, w których do sieci ofiary wprowadzana jest tylna furtka (tzw. backdoor) w celu ustanowienia zdalnego dostępu. W innych przypadkach ofiary infekuje się różnymi rodzajami oprogramowania szpiegującego. Również ataki phishingowe często opierają się na zainfekowanych załącznikach lub zawierają łącze do specjalnie spreparowanej witryny internetowej zainfekowanej złośliwym oprogramowaniem.

> *W przypadku ukierunkowanych lub zaawansowanych cyberataków nie wystarczy polegać wyłącznie na rutynowych skanach antywirusowych, złośliwy kod musi zostać bardziej szczegółowo przeanalizowany.*

Powody, dla których możesz potrzebować bardziej szczegółowej analizy złośliwego oprogramowania

- Ukierunkowany lub zaawansowany cyberatak
- Stosunkowo nowa lub nieznana próbka złośliwego oprogramowania, która pozostaje niewykryta przez standardowe antywirusy
- Aby ocenić ryzyko i potencjalne skutki ataku, należy zidentyfikować wszystkie funkcje, możliwości i konfigurację próbki złośliwego oprogramowania
- Identyfikacja podobnych ataków i kampanii. Planowanie i gotowość na kolejne kroki hakerów
- Dane dotyczące zagrożeń lub dane wywiadu ukierunkowane na klienta
- Identyfikacja i usuwanie wszelkich plików stworzonych przez złośliwe oprogramowanie bez konieczności ponownej instalacji systemu operacyjnego; szczególnie w przypadkach, gdy standardowe antywirusy wykryły tyl-ko niewielką część plików lub w ogóle ich nie wykryły

Usługa analizy złośliwego oprogramowania

- Analiza statyczna i behawioralna - identyfikacja typu
- i rodziny złośliwego oprogramowania, jego podstawowych cech i zachowań
- Tworzenie listy wskaźników naruszenia integralności systemu (IOC), które mogą być wykorzystane podczas reagowania na incydenty, analizy kryminalistycznej, monitorowania zagrożeń i ich aktywnego wyszukiwania
- Ustalenie, czy próbka złośliwego oprogramowania została dostosowana do konkretnej ofiary, czy jest częścią standardowych kampanii masowych
- Ekstrakcja konfiguracji (jeśli dotyczy)
- Analiza cech i identyfikacja funkcjonalności złośliwego oprogramowania
- Przypisanie złośliwego kodu podmiotowi lub kampanii stanowiącej zagrożenie (jeśli to możliwe)
- Zaawansowana analiza złośliwego oprogramowania i inżynieria wsteczna - pełna analiza cech i funkcjonalności, w tym omijanie technik zaciemniania i ochrony przed analizą. Badanie podobnych i/lub powiązanych przypadków, malware intelligence
- Opracowanie specjalnych programów do zaszczepiania, które zapobiegają infekcji próbkami złośliwego oprogramowania użytymi podczas cyberataku
- Opracowanie specjalnych programów i narzędzi do usuwania, które usuwają wszelkie ślady utworzone przez złośliwe oprogramowanie podczas cyberataku

IstroSec

Arkusz danych

Dlaczego IstroSec?

Doświadczenie i wiedza

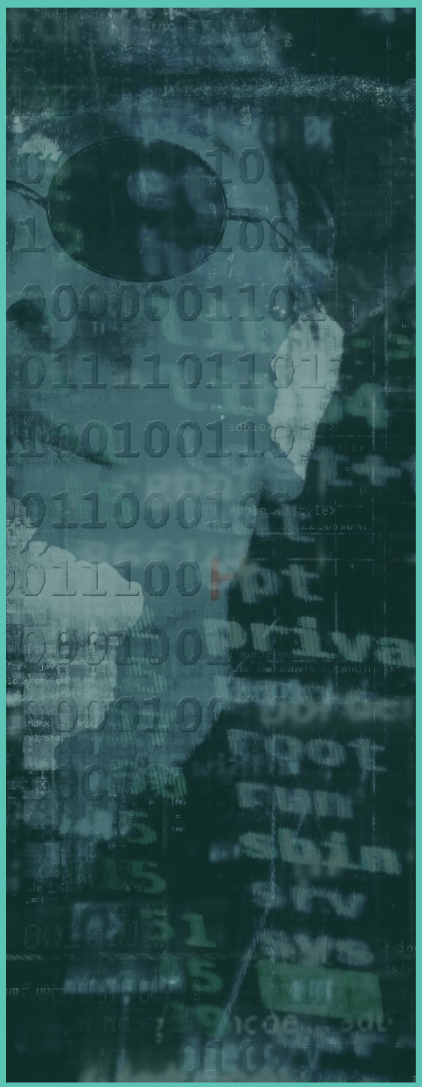
Nasi certyfikowani eksperci posiadają wieloletnie doświadczenie. Przeanalizowali setki próbek złośliwego oprogramowania, w tym próbki wykorzystywane w zaawansowanych i ukierunkowanych atakach cybernetycznych oraz atakach APT na rządowe i globalne firmy. Znają taktykę, techniki i procedury atakujących oraz posiadają niezbędną wiedzę, aby podejmować decyzje oparte na danych na podstawie analizy złośliwego oprogramowania wdrożonego podczas incydentu.

Specjalizacja w analizie złośliwego oprogramowania

Oprócz analizy złośliwego oprogramowania nasi eksperci przeprowadzają również własne badania w zakresie złośliwego oprogramowania oraz szkolenia dotyczące prewencji i threat intelligence. Opracowali również kilka społecznościowych narzędzi typu open source i opublikowali swoje wyniki w wielu artykułach, studiach przypadków i konferencjach w Europie i Stanach Zjednoczonych, w tym DEFCON i BlackHat. Czterech naszych ekspertów było częścią zwycięskiego zespołu LockedShields 2016.

Certyfikowani profesjonaliści

Eksperci IstroSec są również posiadaczami uznanych na całym świecie certyfikatów w tych dziedzinach. Posiadamy certyfikaty takie jak Certified Information Systems Security Professional (CISSP), Certified Information System Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) i inne.



Studium przypadku

Rodzaj firmy: Rządowa
Usługa: Analiza złośliwego oprogramowania
Rozwiązanie: Zaawansowana analiza złośliwego oprogramowania, badanie powiązanych zagrożeń, tworzenie IOC

Nasi badacze znaleźli próbkę złośliwego oprogramowania zamaskowaną jako dokument pochodzący z jednej instytucji rządowej. Analiza złośliwego oprogramowania ujawniła kampanię phishingową, która zaraża ofiary narzędziem Cobalt Strike. Jest ono często używane przez testerów penetracyjnych, a także zaawansowanych atakujących w celu przejęcia kontroli i zdalnego dostępu do zaatakowanych urządzeń.
Na podstawie wyodrębnionej konfiguracji Cobalt Strike nasi analitycy znaleźli serwer sterowania i kontroli. Dzięki danym z malware intelligence znaleźli więcej serwerów, które zostały użyte w atakach na rząd lub zostały przygotowane przez atakujących na przyszłe ataki w ramach tej kampanii. Dostarczyliśmy IOC do rządowego zespołu CSIRT w tym kraju. Dzięki temu możliwe było wykrycie kolejnych ofiar atakujących i zapobieżenie dalszym atakom przy użyciu ujawnionej infrastruktury operacyjnej atakującego.

Rodzaj firmy: Duża komercyjna firma deweloperska IT
Usługa: Analiza złośliwego oprogramowania (+analiza kryminalistyczna i reakcja na incydenty)
Rozwiązanie: Zaawansowana analiza złośliwego oprogramowania, malware intelligence, opracowanie narzędzia do usuwania złośliwych plików

Urządzenia będące w posiadaniu klienta zostały dotknięte nietypowo dużym obciążeniem procesora. Było to spowodowane uruchamianiem procesów zamaskowanych jako niektóre usługi systemu Windows. Usługi te nie były jednak sfałszowane. Kontrola antywirusowa wykryła niektóre z nich jako kopalnie kryptowalut, ale ich usunięcie nie powiodło się - wkrótce zostały utworzone ponownie. Analiza złośliwego oprogramowania zidentyfikowała kilka technik utrwalania używanych przez to złośliwe oprogramowanie. Po przeprowadzeniu badań dotyczących złośliwego oprogramowania analitycy odkryli więcej szkodliwych plików wykorzystywanych w tym ataku, ale już usuniętych przez atakujących. Dzięki wiedzy o tych plikach analitycy byli w stanie zrekonstruować wszystkie etapy ataku. Zidentyfikowali również początkowy dostęp atakujących - wykorzystanie luki w zabezpieczeniach aplikacji internetowej. Następnie opracowali narzędzie do usuwania wszystkich złośliwych plików, wszelkich pozostałości i kilku luk typu backdoor. Dzięki danym z threat intelligence analitycy zna-leźli inne podobne ataki i oszacowali wielkość tej globalnej kampanii oraz zysk atakujących.