Sigurnosne prijetnje na Internetu

Kriminalna skupina Conti

Karlo Baljak, 30.10.2024

Pregled predavanja

- Osnovni pojmovi
- Conti grupa – pregled
- Conti i Rusija
- Organizacija grupe
- Tijek napada
- Conti ransomware
- Pregovori
- Dešifriranje
- Poznati napadi

Pitanja za ispite

1. Objasnite model dvostruke prijetnje kod skupine Conti (eng. double extortion)?
2. Koji je potez Conti grupe uzrokovao curenje informacija o samoj grupi, njezinoj organizaciji i djelovanju?
3. Kako izgleda tijek napada grupe Conti, nabrojite korake?
4. Koje su najčešće korištene biblioteke u pozivima prema kernel APIu koje koristi Conti ransomware?
5. Koje korake prolazi alat za dešifiranje kako bi dešifrirao datoteke?

Odgovori:
1) Model dvostruke prijetnje kod skupine Conti se odnosi na traženje prve otkupnine za dostavljanje ključa za dešifriranje te druge otkupnine kako skupina ne bi objavila pokradene podatke
2) podržavanje Ruske invazije Ukrajine u veljači 2022.
3) Napad se sastoji od 5 koraka: infekcija, inicijalni pristup, istraživanje mreže, izvlačenje podataka i pokretanje ransomwarea
4) KERNEL32.dll, ADVAPI32.dll, WS2_32.dll
5) Alat prolazi kroz 5 koraka: očitavanje originalne veličine datoteke, izvlačenje šifiranog ključa za šifriranje iz datoteke, dešifiranje šifiranog ključa za šifiranje, očitavanje načina šifriranja i na kraju dešifriranje same datoteke

Motivacija (1)

- kibernetičke kriminalne grupe, poput Contija, predstavljaju ozbiljnu prijetnju globalnoj sigurnosti, posebno kada napadaju kritične infrastrukture
- razumijevanje načina na koji djeluju omogućava bolje strategije obrane i reakcije na buduće napade

Motivacija (2)

- veliki je problem što postoji jako malo ili uopće ne postoji dovoljno informacija
- nepoznati načini na koje oni funkcioniraju
- teško saznati bilo što

Osnovni pojmovi

- Ransomware - vrsta štetne programske potpore koja blokira pristup računalu ili svim datotekama
- RaaS - Ransomware-as-a-Service je poslovni model kibernetičkog kriminala u kojem ransomware developeri prodaju svoj ransomware ili malware naručiteljima
- C2 (Command and Control, C&C) – poslužitelj na kojeg se inficirano računalo spaja te sluša naredbe direktno od napadača ili šalje podatke i informacije o sustavu.

Ransomware - vrsta štetne programske potpore koja blokira pristup računalu ili svim datotekama. To su dva načina na koje ransomware može djelovati na računalu žrtve. Prvi, onemogućuje uopće pristup računalu te samo prikazuje poruku koliko treba platiti otkupnine i na koji kripto račun ju poslati. Drugi je način šifriranje svih datoteka na računalu te najčešće se unutar svake mape stvori datoteka s porukom da je računalo inficirano i da treba platiti otkupninu kako bi se dobio ključ za dešifriranje. Plaća se putem kriptovaluta pošto one najviše čuvaju anonimnost.

RaaS - Ransomware-as-a-Service je poslovni model kibernetičkog kriminala u kojem ransomware developeri prodaju svoj ransomware ili malware naručiteljima. Ti naručitelji onda izvode napade, a proizvođači ransomwarea ili malwarea dobivaj određeni udio otkupnine

C2 (Command and Control, C&C) – poslužitelj na kojeg se inficirano računalo spaja te sluša naredbe direktno od napadača ili šalje podatke i informacije o sustavu.

Conti grupa – pregled

- Rusija
- nasljednik grupe WIZARD SPIDER
- model dvostruke prijetnje (eng. double extortion)
- mete: tvrtke, vlade i kritična infrastruktura
- motivacija: novac i politika

Država porijekla ili država iz koje je ova grupa djelovala je Rusija.

Smatra se nasljednikom grupe WIZARD SPIDER i njihovog ransomwarea Ryuk, zbog velikih sličnosti djelovanja.

Model dvostruke prijetnje. To je model u kojem se prvo šifriraju sve datoteke a potom, se prijeti sa objavljivanjem svih pokradenih datoteka. Ovaj model nije nova pojava, takav model su koristile i grupe REvil, MAZE, Ragnar, Egregor.

Mete napada ove grupe su tvrtke, vlade i vladine institucije te kritične infrastrukture svih zemalja svijeta s naglaskom na SAD. Samo od 01/01/2021 pa do 12/11/2021 bilo je 1.6 mil. napada na tvrtke u SAD-u, a druga država po broju napada je Nizozemska sa 49000 napada

Motivacije za napade ove grupe su novac i politički razlozi koji se usko poklapaju sa političkim idejama Rusije. Najveće otkupnine koje su zabilježene sežu do 25 mil. dolara

Conti i Rusija

- podupiru Rusku invaziju Ukraijne, loš potez?
- uska suradnja sa Ruskim APT-om?
- zašto Rusija?

Grupa Conti je u veljači 2022, kada je Rusija pokrenula invaziju na Ukrajinu, javnom izjavom poduprla Rusiju. Obavještajni rad organizacije Advanced Intel u svibnju 2022. navodi kako je ta javna izjava bila puno više nego sama izjava. Od toga dana Conti grupa nije primila nikakvu otkupninu. Plaćanje otkupnine je nestalo zbog sankcija koje je SAD pokrenuo.

Također se postavlja pitanje djeluje li skupina Conti u uskoj suradnji s Ruskim APT-om, pošto Conti također napada kritične infrastrukture i nema nikakvih moralnih dilema oko takvih napada.

Zašto Rusija? Rusija dopušta takvim grupa poprilično slobodno djelovanje sve dok se napadači ne okreću protiv države i njezinih institucija. Takve grupe razvijaju svoje viruse na način da virus prvo saznaje u kojoj se mreži ili sustavu nalazi te ukoliko otkrije da se nalazi unutar sustava ili područja pod Ruskom kontrolom, tj. u području Russian Commonwealth States (CIS), istog se trena gasi i prestaje s radom).

Organizacija grupe

- organizacija u standardima velikih tvrtki
- odjeli imaju budžet, osoblje i upravu
- odjeli za: testiranje, traženje ranjivosti, iskorištavanje ranjivosti, uspostavljanje infrastrukture za napad
- 5 radnih dana, od 10-11h do 19h

 @ContiLeaks

Do informacija o organizaciji grupe i kako ona funkcionira se došlo analizom procurenih informacija koje je objavio nepoznati X korisnik sa korisničkim imenom @ContiLeaks (https://x.com/contileaks?lang=en). Kasnije je bilo puno istraživača i IT specijalista koji su uz pomoć NLPa (natural language processing) i LDAa (Latent dirichlet allocation) analizirali sve informacije i povijest poruka sa servera s koji je korisnik @ContiLeaks objavio razgovore članova grupe Conti. Tako saznajemo neke zanimljivosti od kojih su neke:

Da grupa Conti ima hijerarhijsku organizaciju. Tvrtka Check Point Software je otkrila kako Conti zapošljava i održava razne odjele kao što su: ljudi resursi, menadžment, financije. Također svi ti odjelu funkcioniraju hijerarhijski, svaki odjel ima svog vođu, te taj vođa odgovara svom vođi itd. Svaki odjel ima svoje osobolje, budžet s kojim raspolaže i nekakvu internu upravu koja odgovara glavnoj upravi.

Neki od odjela koji nisu uobičajeni u normalnim tvrtkama, tj. tvrtkama koje se bave legalnim poslovima:
1) Testeri ransomwarea/malwarea - umjesto testera za greške u kodu, Conti ima testere koji provjeravaju prolazi li njihov šteni kod ispod radara svim antivirusima, IDS-evima. Također jedan od poslaova testera je i obfuscirati kod
2) Traženje ranjivosti - Poseban odjeli za pronalaženje ranjivosti operativnih sustava i aplikacija

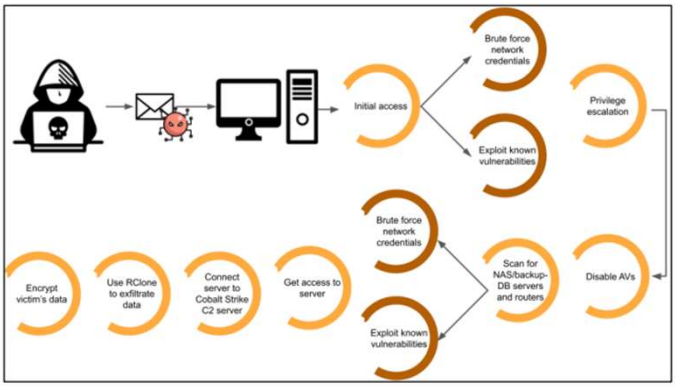
3) Iskorištavanje ranjivosti - izgradnja napadačkog plana oko pronađene ranjivosti
4) Uspostavljanje infrastrukture – uspostava C2 poslužitelja i druge potrebne infrastrukture za izvršavanje osmišljenog plana napada, glavni način distribuiranja Conti štetne programske podrške, i sakupljanja ukradenih datoteka

Tijek napada (1)

1. Infekcija
2. Inicijalni pristup
3. Istraživanje mreže
4. Izvlačenje podataka
5. Pokretanje ransomwarea

Način na koji Conti napada svoje žrtve se može u grubo podijeliti u 5 koraka: Infekcija, Inicijalni pristup, Istraživanje mreže, Izvlačenje podataka, Pokretanje Conti ransomwarea

Tijek napada (2)



Slika 1. Team Cymru "Analyzing ransomware negotiations with CONTI: An in-depth analysis" Figure 1

Na slici se to može vidjeti

Tijek napada (3) - Infekcija

- socijalni inženjering
- ljudska greška
- phishing mailovi

Najčešći razlog upadanja u sustave je ljudska greška. Najvažnije je pronaći dovoljno informacija o osobi koju se cilja iskoristiti da bi se dobio pristup sustavu. To je uglavnom osoba na visokoj poziciji ili s puno ovlasti u sustavu. Zahvaljujući današnjim društvenim mrežama i ljudskoj nepažnji, lako se saznaju informacije koje bi se mogle iskoristiti kako bi se namamilo takvu osobu i kompromitirao njezin račun.

Tijek napada (4) – Inicijalni pristup

- slabosti RDPa, Microsoft Exchangea, vatrozida, Apache Log4j
- Windows Printer Spooler servis (PrintNightmare)
- Zerologon
- FortiGate

Inicijalnim pristupom napadač ispred sebe ima cijeli inficirani sustav na pladnju. U tom trenutku može istraživati servise koji se na njemu vrte i tražiti poznate slabosti. Često korištene slabosti su slabost Remoto Desktop Protocola (RDPa), Microsoft Exchangea, loše postavljenog vatrozida, Apache Log4j. Napad na Windows Printer Spooler servis još poznat pod imenom PrintNightmare, koji omogućava remote code execution pod SYSTEM privilegijama. Zerologon je ranjivost Netlogon Windows Server procesa koji inače autentificira korisnike unutar neke domene te se može iskoristiti kao sustav za otvaranje skrivenog kanala za komunikaciju. FortiGate: path traversal ranjivost u Fortinetovom FortiGate SSL VPNu te omogućuje čitanje datoteka računala udaljeno sa specijalno napravljenim zahtjevom. Nakon što sustav dođe pod kontrolu napadača ili napadač dobije veće ovlasti od samo korisnika sustava, kreće sa isključivanjem antivirusa, IDSa.

Tijek napada (5) – Istraživanje mreže

- Net i ADFind
- izrada topologije
- pronalazak poslužitelja sa sigurnosnim kopijama

Net i ADFind su Windows naredbe/alati pomoću kojih Conti dolazi do podataka u aktivnom direktoriju, tj. vjerodajnicama korisnika sustava. Istražuje mrežu i podmreže te gradi informatičku verziju „umne" mape kako bi kasnije bilo jednostavnije za navigirati. Tijekom istraživanja mreže traži poslužitelje na kojima se čuvaju sigurnosne kopije.

Tijek napada (6) - Eksfiltracija podataka

- CobaltStrike
- RClone

Kada se otkrije lokacija poslužitelja sa potencijalno korisnim podacima za napadača, Conti koristi CobaltStrike alat kako bi ubacio ostale alate ili programe koji su potrebni za daljnji tijek napada, CobaltStrike je zapravo dropper. RClone je jedan od tih alata koje CobaltStrike ubaci u sustav, te pomoću njega se podaci kopiraju na C2 poslužitelj napadača.

Tijek napada (7) – Pokretanje ransomwarea

- pokrene se jedna exe datoteka
- do 32 dretve
- asimetrično šifriranje
- datoteke dobivaju nastavak .CONTI
  - (ili .6P5CL, .ODMUA, .YZXXX, .LSNWX, .TJODT)
- poruke u mapama

Instalira se u obliku izvršne datoteke koja ima ulogu loadera i DLLa. Zanimljivo je zašto samo jedna datoteka? Jedna je datoteka kako bi se tijekom izvođenja program mogao sam sebe referencirati, na taj su način uključeni svi procesi na sustavu.

Pokreću se do 32 dretve ransomwarea zbog bržeg i efikasnijeg šifriranja svih datoteka na sustavu.

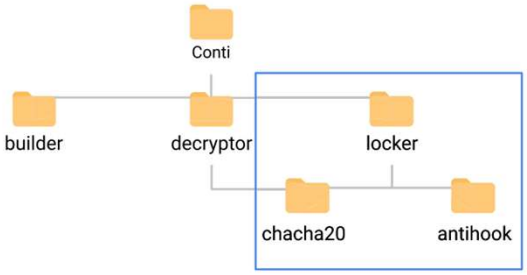
Asimetrično šifriranje – koristi se par javnog i privatnog ključa. Javni ključ Contia je zapisan u samom ransomwareu, a privatni se ključ čuva na sigurnom kod Contia

Datoteke nakon što su šifrirane dobivaju nastavak .CONTI ili .6P5CL, .ODMUA, .YZXXX, .LSNWX, .TJODT ovisno o verziji ransomwarea.

Kada ransomware šifrira sve datoteke unutar mape, uvijek ostavlja poruku (README) unutar koje se nalazi poruka da je sustav pod napadom Conti ransomwarea i da su svi podaci šifrirani te su napisane instrukcije kako dalje postupati, ali o tome na idućem slajdu.

Conti ransomware (1)

- verzija 3
- prodaje se pod RaaS modelom
- jezik: C++
- ciljani operativni sustav:
  - Windows 10



Slika 2. Istraživački članak "An Analysis Of Conti Ransomware Leaked Source Codes", Saleh Alzahrani, Yang Xiao, Wei Sun, Figure 2

Među svim porukama koje je objavio X korisnik @ContiLeaks, bio je i objavljen izvorni kod ransomwarea verzije 3. Zahvaljujući tome napravljene su detaljne statičke i dinamičke analize ransomwarea. Kroz koje ću ja sada proći.

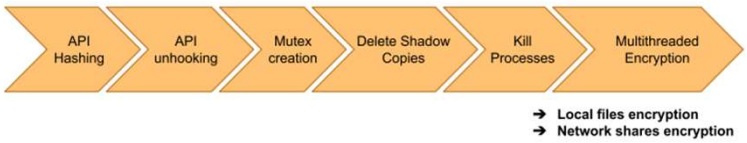
Analizirana je verzija 3 ransomwarea.

Ovaj se ransomware prodaje pod RaaS modelom što znači da je vrlo fleksibilan i lako prilagodljiv za potrebe različitih naručitelja.

Sami je ransomware pisan u C++ te proučena verzija je napadala sustave s Windows 10 operativnim sustavom.

Na slici 2 moguće je vidjeti strukturu Conti ransomwarea projekta.

Conti ransomware (2)



Slika 3. Istraživački članak "An Analysis Of Conti Ransomware Leaked Source Codes", Saleh Alzahrani, Yang Xiao, Wei Sun, Figure 3

Encryption method	Targeted Files
Full Encryption	• Database files with following extensions: .4dd, .4dl, .accdb, .accde, .accde, .acedr, .accdt, .accft, .adb, .ade, .adf, .adp, .arc, .ora, .alf, .ask, .btr, .bdf, .cat, .cdb, .ckp, .cma, .cpd, .dacpac, .dad, .dadiagrams, .daschema, .db, .db-shm, .db-wal, .db3, .dbc, .dbf, .dbs, .dbt, .dbv, .dbx, .dcb, .dct, .dcx, .ddl, .dlis, .dp1, .dqy, .dsk, .dsn, .dtsx, .dxl, .eco, .ecx, .edb, .epim, .exb, .fcd, .fdb, .fic, .fmp, .fmp12, .fmpsl, .fol, .fp3, .fp4, .fp5, .fp7, .fpt, .frm, .gdb, .grdb, .gwi, .hdb, .his, .ib, .idb, .ihx, .itdb, .itw, .jet, .jtx, .kdb, .kexi, .kexic, .kexis, .lgc, .lwx, .maf, .maq, .mar, .mas.mav, .mdb, .mdf, .mpd, .mrg, .mud, .mwb, .myd, .ndf, .nnt, .nrmlib, .ns2, .ns3,.ns4, .nsf, .nv, .nv2, .nwdb, .nyf, .odb, .ogy, .orx, .owc, .p96, .p97, .pan, .pdb, .p dm, .pnz, .qry, .qvd, .rbf, .rctd, .rod, .rodx, .rpd, .rsd, .sas7bdat, .sbf, .scx, .sdb, .sdc, .sdf, .sis, .spg, .sql, .sqlite, .sqlite3, .sqlitedb, .te, .temx, .tmd, .tps, .trc, .trm, .udb, .udl, .usr, .v12, .vis, .vpd, .vvv, .wdb, .wmdb, .wrk, .xdb, .xld, .xmlff, .abcddb, .abs, .abx, .accdw, .adn, .db2, .fm5, .hjt, .icg, .icr, .kdb, .lut, .maw, .mdn, .mdt • File size is lower than 1,04 MB
Header Encryption	• File size is between 1,04 MB and 5,24 MB
Partial Encryption	• Virtual Machines files with following extensions: .vdi, .vhd, .vmdk, .pvm, .vmem, .vmsn, .vmsd, .nvram, .vmx, .raw, .qcow2, .subvol, .bin, .vsv, .avhd, .vmrs, .vhdx, .avdx, .vmcx, .iso • File size greater than 5,24 MB

Slika 4. Istraživački članak "An Analysis Of Conti Ransomware Leaked Source Codes", Saleh Alzahrani, Yang Xiao, Wei Sun, Table 3

#	Argument value	Name	Value	Description	Notes
1	all	ALL_ENCRYPT	10	Encrypt both local and network shared files	Default mode
2	local	LOCAL_ENCRYPT	11	Encrypt only local files	
3	net	NETWORK_ENCRYPT	12	Encrypt only network shared files	
4	backups	BACKUPS_ENCRYPT	13	Encrypt only backup files	Not implemented

Slika 5. Istraživački članak "An Analysis Of Conti Ransomware Leaked Source Codes", Saleh Alzahrani, Yang Xiao, Wei Sun, Table 2

Tijek izvršavanja ransomwarea je vidljiv na slici 3. Možemo ga podijeliti u 6 koraka:

1. izrada sažetka APIa – služi kako bi se obfuscirala imena pozivajućih APIa i biblioteka koje ih pružaju. To je napravljeno kako bi se prikrile funkcionalnosti programa od statičke analize i skenera zloćudnog koda na osnovi učestalih uzoraka. Time napadač obfuscira nazive, a ransomware ih tijekom rada sam deobfuscira.

2. API-unhooking – mehanizam kojim se zaobilazi stvarno-vremena zaštita od EDR ili modernih AV-ova, na način da uspoređuje verziju biblioteke u memoriji i onu na disku i zamijeni „zakvačene" oktete u memoriji sa onima na disku

3. Stvaranje mutexa – osigurava da je u jednom trenutku samo jedna instanca ransomwarea aktivna

4. Brisanje Shadow kopija - onemogućava sve mogućnosti oporavka sustava. Time, kada dođe do šifriranja, sve sigurnosne kopije koje nisu pospremljene offline će biti beskorisne.

5. Gašenje svih procesa – pokušava pogasiti sve procese, kako bi mogao šifrirati sve njihove podatke

6. višedretveno šifriranje datoteka – ovisno o kakvoj se datoteci radi i njezinoj veličini ransomware će na drugačiji način šifrirati svaku datoteku, vidljivo na slikama 4. i 5.

Conti ransomware (3)

- KERNEL32.dll
- WS2_32.dll
- ADVAPI32.dll

DLL	HASH	API function	DLL	HASH	API function
KERNEL32.dll	0xbc3d21a8	LoadLibraryA	KERNEL32.dll	0xa62cc8e1	SetFileAttributesW
KERNEL32.dll	0x19515ab5	CancelIo	KERNEL32.dll	0x2ffbe59f	lstrlenW
KERNEL32.dll	0x55710126	GlobalAlloc	KERNEL32.dll	0xc65c5ee6	lstrlenA
KERNEL32.dll	0xf91ac9a0	ReadFile	KERNEL32.dll	0x1b1acbcc	GetFileSizeEx
KERNEL32.dll	0x663b63f4	GetCurrentProcess	KERNEL32.dll	0xc45f4a8c	WriteFile
KERNEL32.dll	0x3ce51c64	HeapFree	KERNEL32.dll	0x31d910df	GetProcessId
KERNEL32.dll	0xede8a61e	SetEndOfFile	KERNEL32.dll	0x6a095e21	WaitForSingleObject
KERNEL32.dll	0xf06e87ca	CreateFileW	KERNEL32.dll	0x93afb23a	GetFileAttributesW
KERNEL32.dll	0x1fbbb84f	GetLastError	KERNEL32.dll	0xf07ba2639	lstrcatW
KERNEL32.dll	0xa5eb6e47	CloseHandle	KERNEL32.dll	0xdf1af05e	GetNativeSystemInfo
KERNEL32.dll	0xd54e6bd3	SetFilePointerEx	KERNEL32.dll	0x7324a0a2	CreateProcessW
KERNEL32.dll	0x4d9702d0	lstrcpyW	KERNEL32.dll	0xc8fb7817	MoveFileW
KERNEL32.dll	0xd52132a3	GetCommandLineW	KERNEL32.dll	0xf701962e	CreateMutexA
KERNEL32.dll	0x3a4532be	CreateThread	KERNEL32.dll	0x0cd05546	MultiByteToWideChar
KERNEL32.dll	0xd72e57a9	lstrcmpiW	KERNEL32.dll	0x21cca665	EnterCriticalSection
KERNEL32.dll	0x263040ab	HeapAlloc	KERNEL32.dll	0xc5e8a09c	GetProcessHeap
KERNEL32.dll	0xaf17f6da	DeleteTimerQueue	KERNEL32.dll	0xf99eabb9	LeaveCriticalSection
KERNEL32.dll	0xb87c8bb7	ExitThread	KERNEL32.dll	0x441bdf1e	PostQueuedCompletionStatus
KERNEL32.dll	0xe4b69f3b	Sleep	KERNEL32.dll	0x1b99344d	GetLogicalDriveStringsW
KERNEL32.dll	0xa0ee5aad	GlobalFree	KERNEL32.dll	0xf4241d9a	DeleteCriticalSection
KERNEL32.dll	0xf05ad6da	CreateTimerQueue	KERNEL32.dll	0x57b499e3	CreateIoCompletionPort
KERNEL32.dll	0xe2b40f85	FindFirstFileW	KERNEL32.dll	0x9aea18e1	FindNextFileW
KERNEL32.dll	0x75fcf770	FindClose	KERNEL32.dll	0x397b11df	lstrcmpW
KERNEL32.dll	0xd827c1e1	VirtualAlloc	KERNEL32.dll	0x1d7ab241	WaitForMultipleObjects
KERNEL32.dll	0x7f0ff14e	GetCurremProcessId	KERNEL32.dll	0xa65b5727	GetModuleHandleW
ADVAPI32.dll	0xa247ff77	CryptImportKey	ADVAPI32.dll	0x6c6c937b	CryptEncrypt
ADVAPI32.dll	0xabcb0a67	CryptGenRandom	ADVAPI32.dll	0x5cc1ccbc	CryptAcquireContextA
NETAPI32.dll	0xa1f2bf63	NetApiBufferFree	NETAPI32.dll	0x1668d771	NetShareEnum
IPHLPAPI.dll	0xbf983c41	GetIpNetTable	SHELL32.dll	0xc7dfa7fc	CommandLineToArgvW
RSTRTMGR.dll	0x7d154065	RmEndSession	RSTRTMGR.dll	0xb5e437b0	RmStartSession
RSTRTMGR.dll	0xbbd8beb8	RmGetList	RSTRTMGR.dll	0x2ad410e3	RmRegisterResources
RSTRTMGR.dll	0x22cb760f	RmShutdown	OLE32.dll	0xd3a7a468	CoUninitialize
OLE32.dll	0xb32feeec	CoCreateInstance	OLE32.dll	0xde5dbfdc	CoSetProxyBlanket
OLE32.dll	0xcc12507f	CoInitializeSecurity	OLE32.dll	0x2bdbdf4e	CoInitializeEx
WS2_32.dll	0xbd6ac662	gethostbyname	WS2_32.dll	0x1260d6db	gethostname
WS2_32.dll	0x00c1575b	socket	WS2_32.dll	0x1ad64c3e	WSAIoctl
WS2_32.dll	0x4118bcd2	closesocket	WS2_32.dll	0x5dacc2ba	WSAAddressToStringW
WS2_32.dll	0xe558706f	WSASocketW	WS2_32.dll	0x4310229a	bind
WS2_32.dll	0x55d15957	setsockopt	WS2_32.dll	0xe34ea561	getsockopt
WS2_32.dll	0x61856121	shutdown	WS2_32.dll	0xaf724aac	WSAStartup
WS2_32.dll	0x9812c1b7	WSACleanup	WS2_32.dll	0x7e2eafb0	InetNtopW
SHLWAPI.dll	0x6877b7f6	StrStrIA	SHLWAPI.dll	0x5a8ce5b8	StrStrIW
KERNEL32.dll	0x87b69cc9	CreateTimerQueueTimer	KERNEL32.dll	0x1972bf90	Wow64DisableWow64FsRedirection
KERNEL32.dll	0x5d48fbaf	InitializeCriticalSection	KERNEL32.dll	0x78ee4dfa	Wow64RevertWow64FsRedirection
KERNEL32.dll	0xcd976938	GetQueuedCompletionStatus			

Najčešće korištene biblioteke u pozivima APIa prema kernelu.

KERNEL32.dll: Upravlja osnovnim funkcijama sustava poput upravljanja memorijom, ulazno/izlaznim operacijama i obradom prekida u Windowsu. Ključan je za većinu programa kako bi mogli komunicirati s hardverom i sistemskim resursima.

WS2_32.dll: Implementira Winsock API (Windows Sockets) koji je odgovoran za mrežnu komunikaciju (TCP/IP). Koriste ga programi koji se povezuju na internet ili komuniciraju preko mreže.

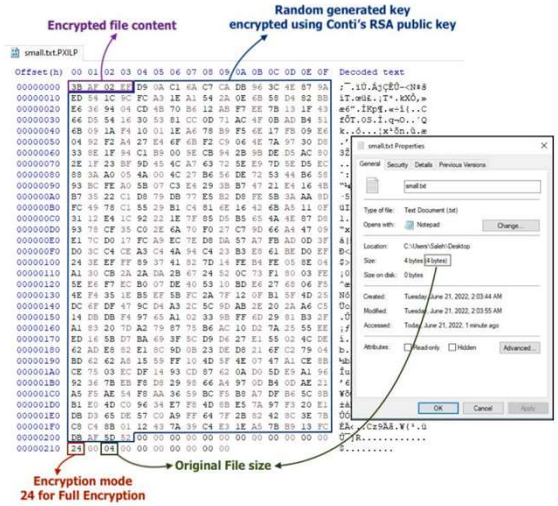
ADVAPI32.dll: Omogućuje napredne API usluge u Windowsu, uključujući funkcionalnosti vezane uz sigurnost poput upravljanja korisničkim računima, servisima, pristupom registru i zapisivanjem događaja.

Conti ransomware (4)

- ChaCha20
  - varijanta Salsa20 algoritma
  - 32 - oktetni ključ
  - 8 – oktetni inicijalizacijski vektor
  - sve se šifrira RSA algoritmom i javnim ključem Contia
  - šifriranje svih datoteka

Generira se 32-oktetni ključ sa 8-oktetnim inicijalizacijskim vektorom, a potom je 32-oktetni ključ šifrira RSA algoritmom i javnim ključem napadača. S tim ključem se onda ovisno o vrsti datoteke i veličini odabire adekvatan način šifriranja prema slikama 4. i 5. na prošlom slajdu.

Šifrirana datoteka



Slika 6. Istraživački članak "An Analysis Of Conti Ransomware Leaked Source Codes", Saleh Alzahrani, Yang Xiao, Wei Sun, Figure 28

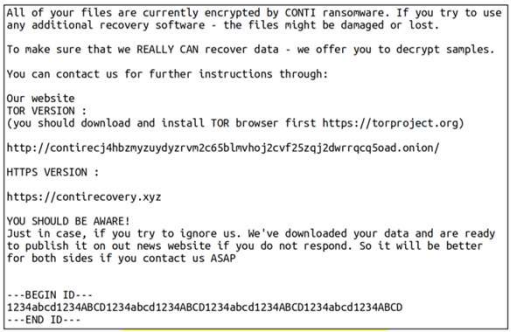
Tu se može vidjeti izgled šifrirana datoteke u hex editoru.

Pregovori (1)

- prije: mail, novije: stranice
- kratki, ali spori pregovori

Slika 8. Team Cymru "Analyzing ransomware negotiations with CONTI: An in-depth analysis" Figure 4

Slika 9. Team Cymru "Analyzing ransomware negotiations with CONTI: An in-depth analysis" Figure 5



```
All of your files are currently encrypted by CONTI ransomware. If you try to use
any additional recovery software - the files might be damaged or lost.

To make sure that we REALLY CAN recover data - we offer you to decrypt samples.

You can contact us for further instructions through:

Our website
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/

HTTPS VERSION :

https://contirecovery.xyz

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded your data and are ready
to publish it on out news website if you do not respond. So it will be better
for both sides if you contact us ASAP


---BEGIN ID---
1234abcd1234ABCD1234abcd1234ABCD1234abcd1234ABCD1234abcd1234ABCD
---END ID---
```

Slika 7. Team Cymru "Analyzing ransomware negotiations with CONTI: An in-depth analysis" Figure 2

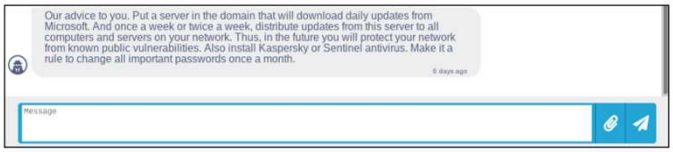
Naklon što je sustav u potpunosti šifriran i korisnik to uoči, jedino što mu preostaje je ili probati učitati offline sigurnosnu kopiju ili postupiti onako kako mu je rečeno u uputama koje je napadač ostavio.

U početku su svi pregovori išli putem maila, a kasnije je grupa Conti razvila stranicu za pregovore koja je bila dostupna i na javnom internetu, a i na TORu, slika 7.

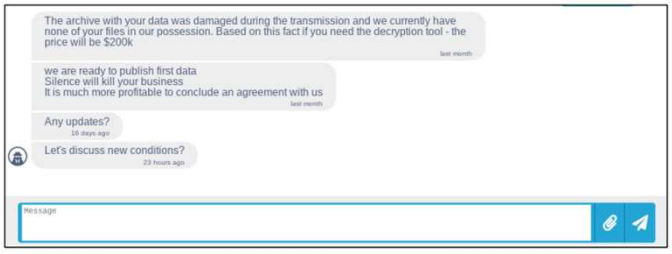
Pregovori su uglavnom vrlo brzi, kroz svega par poruka, ali znaju trajati dosta dugo po nekoliko tjedana, dugo vrijeme da Conti odgovori.

Postavljanje README.TXT (vidimo kako se na stranici, od žrtve traži da postavi datoteku u kojoj navodi tko je i u ime koje se firme ili institucije javlja te da priloži svoj ID koji joj je generiran u datoteci s uputama. Slike 8. i 9.

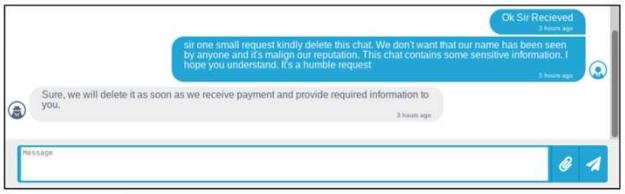
Pregovori (2)



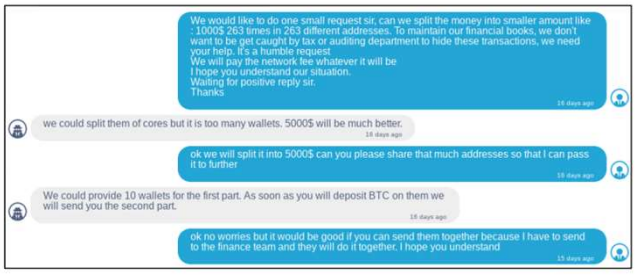
Slika 10. Team Cymru "Analyzing ransomware negotiations with CONTI: An in-depth analysis" Figure 8



Slika 11. Team Cymru "Analyzing ransomware negotiations with CONTI: An in-depth analysis" Figure 9



Slika 12. Team Cymru "Analyzing ransomware negotiations with CONTI: An in-depth analysis" Figure 11



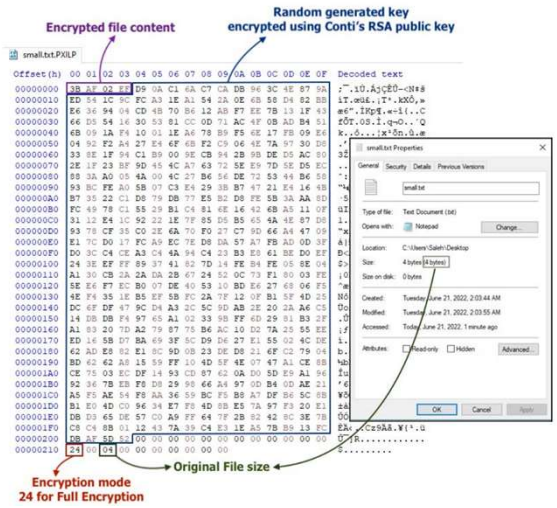
Slika 13. Team Cymru "Analyzing ransomware negotiations with CONTI: An in-depth analysis" Figure 10

Profesionalni i prijateljski pristup (Pružaju savjete što napraviti kako ne bi došlo do sličnog incidenta (Slika 10. i Slika 11.), pa čak i priznaju greške sa svoje strane.

Voljni su čak i uvažiti molbe žrtvi (Slika 12. i Slika 13.)

Dešifriranje

- Conti alatom za dešifriranje
- 5 koraka:
  1. čitanje veličine datoteke
  2. izvlačenje ključa
  3. dešifriranje ključa privatnim ključem
  4. očitavanje načina šifriranja
  5. dešifriranje cijele datoteke



Nakon uspješnog pregovora i plaćanja otkupnine, žrtva alat za dešifriranje od Contia. Kako bi se datoteka u potpunosti dešifrirala potrebno je sljedećih 5 koraka:

1) očitavanje veličine datoteke - kako bi se mogao izvući šifrirani ključ za šifriranje
2) izvlačenje ključa za šifriranje iz šifrirane datoteke
3) dešifriranje tog ključa privatnim ključem Contia kako bi se došlo do stvarnog ključa kojim je šifrirana datoteka
4) očita se način šifriranja koji je korišten (full, header ili partial)
5) dešifriranim ključem za šifriranje i načinom šifriranja se datoteka dešifrira u cijelosti

Napadi

- Ireland's Healthcare Services Executive (HSE)
- vlada Kostarike

Healthcare Service Executive napad

- Irski zdravstveni sustav
- motiv: zarada
- ožujak 2021. – svibanj 2021.
- inicijalni pristup putem web aplikacije sa ukradenim vjerodajnicama
- širenje mrežom
- detonacija ransomwarea

Sustav koji pruža javnu zdravstvenu uslugu na skoro 4000 lokacija i 58 bolnica diljem Irske

Kao što je prije navedeno, ova grupa je financijski motivirana, a bolnice i zdravstvo je područje koje će uvijek platiti novac, kako bi što prije krenulo dalje s radom pošto je to kritična infrastruktura.

Početak napada i upadanja u sustav, ožujak 2021., gibanje po sustavu, eksfiltracija podataka sve do detonacije 14/05/2021.

Do vjerodajnica je grupa došla pomoću phishing mail-a, koji je u sebi sadržavao dokument sa makroima. Otvaranjem dokumenta su se pokrenuli makroi i ostvarili vezu prema Conti C2 serveru.

Nakon inicijalnog ulaza u sustav, Conti je dalje dobio pristup ostalim dijelovima mreže i u kratkom roku došao do cijelog HSE IT sustava. Tako su u sustavu ostali neotkriveni skoro 8 tjedana. Tijekom tih 8 tjedana su probijali račune, pokušavali doći do administratorskih računa, podizali razinu ovlasti, pokrali medicinske podatke sa servera brojnih bolnica.

Nakon 8 tjedan izvlačenja tih podataka, Conti je preko C2 poslao svoj ransomware i pokrenuo šifriranje cijelog HSE IT sustava. Obustavljeni apsolutno svi servisi i usluge, od telekomunikacije prema javnom zdravstvu, komunikacije putem maila, pa čak i hitne službe. HSE je odbio platiti traženu otkupninu i od PricewaterhouseCoopers (PWC) zatražio sanaciju štete. Tek 09/09/2021. PWC je uspješno dešifrirao sve šifrirane podatke i osposobio sustav nazad u normalu.

Napad na vladu Kostarike

- motiv: "srušiti vladu korištenjem kibernetičkog napada„
- stvarni motiv?
- 10.04.2022
- 27 agencija, Ministarstvo financija
- onesposobljena internacionalna trgovina
- pokušaj iskorištavanja državljana

Grupa Conti je za motiv ovog napada izjavila kako oni žele srušiti vladu korištenjem kibernetičkog napada.

Najvjerojatnije prekriti trenutačni, u tom vremenu, raspad grupe Conti i osnivanje nove grupe HIVE.

Napad na upravljajuća tijela Kostarike (čak 27 agencija, među kojima se našlo i Ministarstvo Financija).

Ogromni kolaps cijelog financijskog sektora Kostarike, lokalna poduzeća su prijavljivala gubitke od 38 milijuna dolara dnevno

Conti je na svojim stranicama i društvenim mrežama nagovarao državljane da prisile vladu na plaćanje otkupnine, no predsjednik Chaves je odbio plaćanje početne otkupnine od 10 mil dolara te je ona samo porasla na 20 mil dolara.

Zaključak

- Conti je jedna od najopasnijih i najprofitabilnijih kibernetičkih kriminalnih grupa
- važno je podići svijest o phishing napadima i kako uočiti što bi mogao biti phishing napad
- važna je dobra organizacija lokalne mreže i kontinuirana provjera aktualnih ranjivosti te popravljanje istih

Literatura (1)

[1] Trendmicro, What is Ryuk ransomware, https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html, pristupljeno 14/10/2024

[2] Team Cymru "Analyzing ransomware negotiations with CONTI: An in-depth analysis„

[3] Gray, Ian W., et al. "Money Over Morals: A Business Analysis of Conti Ransomware." 2022 APWG Symposium on Electronic Crime Research (eCrime). IEEE, 2022.

[4] Ruellan, Estelle, Masarah Paquet-Clouston, and Sebastian Garcia. "Conti Inc.: Understanding the Internal Discussions of a large Ransomware-as-a-Service Operator with Machine Learning." arXiv preprint arXiv:2308.16061 (2023).

[5] Williams, Kameron A. Conti Ransomware Gang: An Analysis of the Group's Motives and Methods. Diss. Utica University, 2022.

Dodatna literatura

Stolk, Valentijn. "You Win Some You Ransom: Reconstructing the ransomware ecosystem using ground truth communication data of the Conti ransomware gang." (2022).

Analiza Conti ransomwarea, VirusTotal, https://www.virustotal.com/gui/file/0737ebb6ede108d90216bc06ccfce57defa2179bfda93a34edd868a6f9172a78/detection, pristupljeno 14/10/2024

Hvala!