UNIONE INDUSTRIALE TORINO

Protocollo di intesa

Vantaggi per gli Associati

Paolo Buttigliengo
Responsabile IT - Unione Industriale Torino

UNIONE INDUSTRIALE TORINO

Agenda

- Introduzione « notizie dal mondo Cyber »
- Come aderire alla newsletter "UI contrast"
- Canale preferenziale per gli associati con la Polizia Postale
- Come leggere un report proveniente dalla Polizia Postale per valutare le notifiche al Garante…

UNIONE INDUSTRIALE TORINO

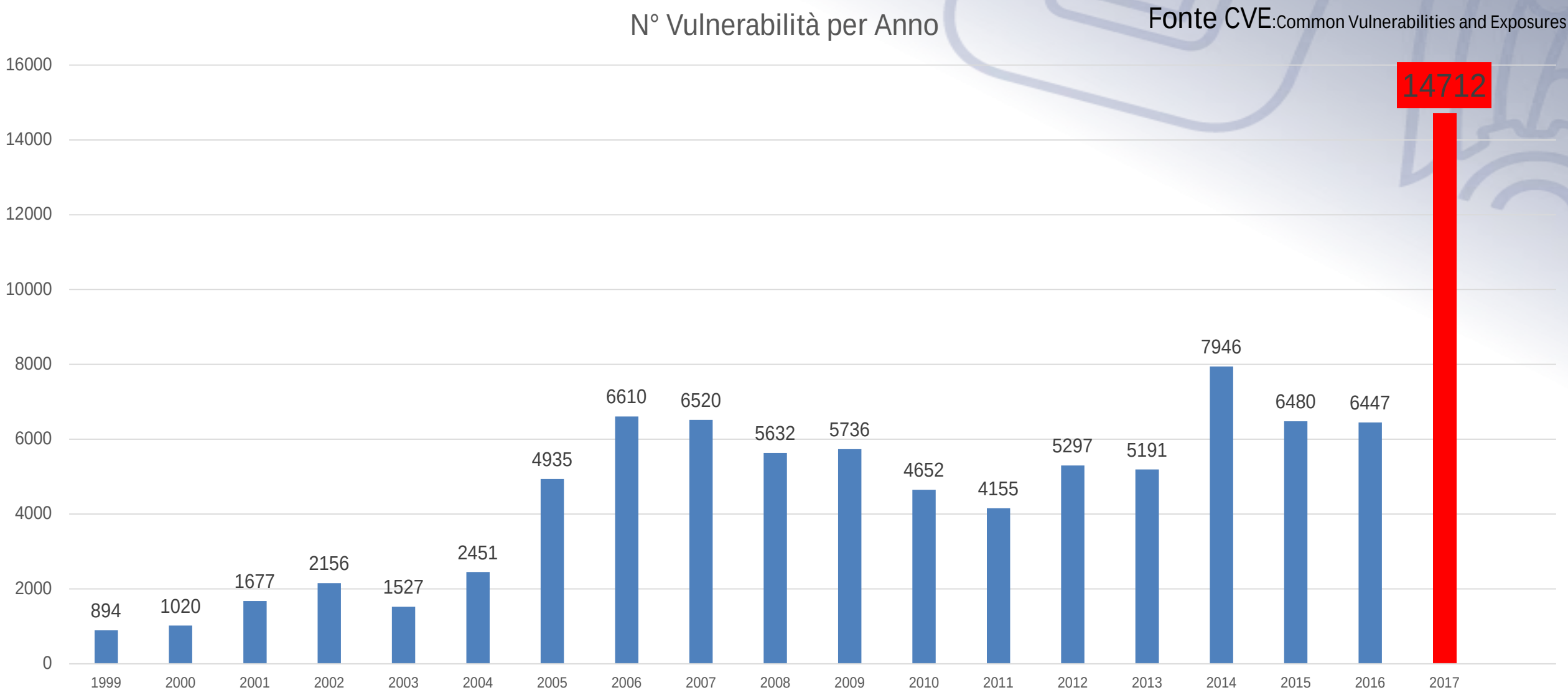
Alcune notizie dal mondo Cyber… lo sapevate che….

- Il Virus WANNACRY è stato scoperto 91 giorni prima della sua «esplosione»
- La patch sulla vulnerabilità utilizzata da questo virus è stata rilasciata 59 giorni prima dell'attacco
- Vi sono state 200000 «vittime» e 300000 pc in 150 nazioni infettati.
- Perdita finanziaria stimata… 4 miliardi $

Bastava aggiornare i pc e i server…

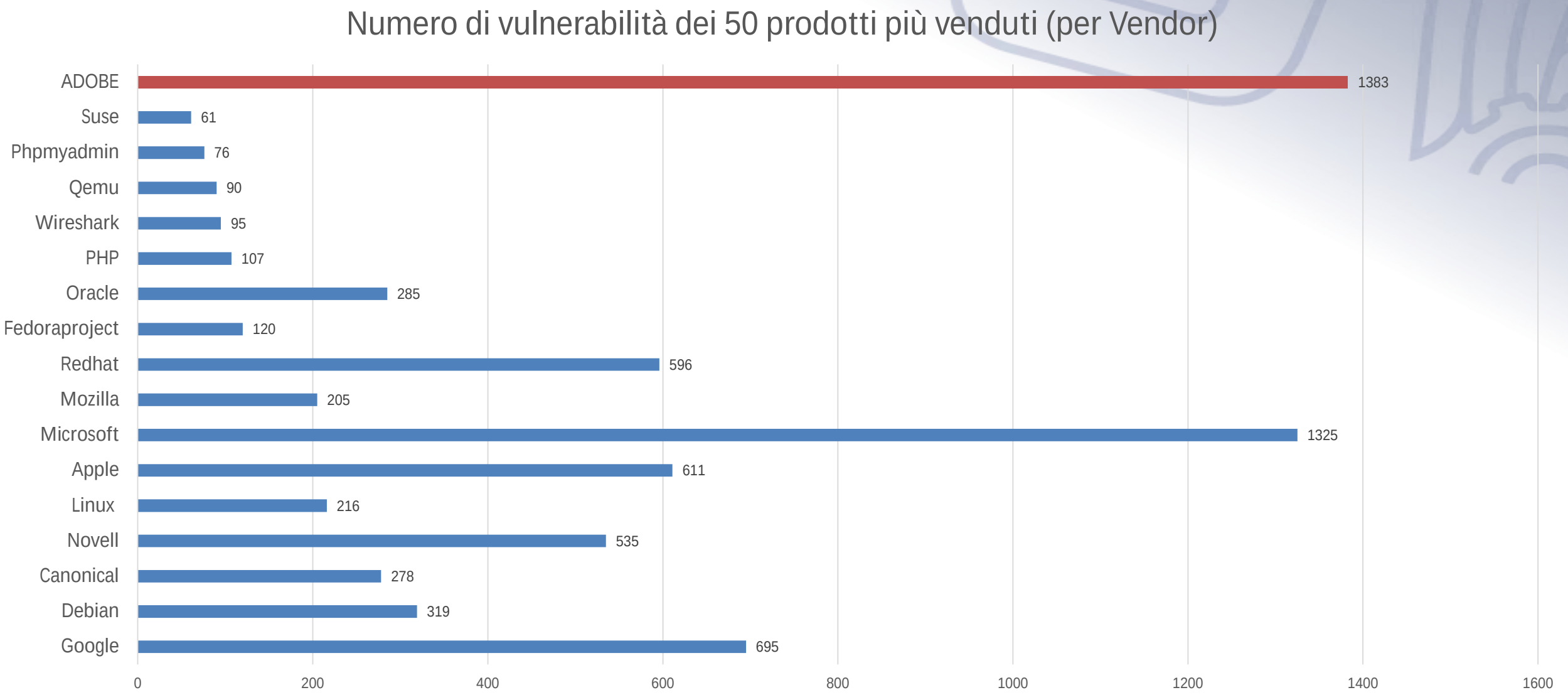
UNIONE INDUSTRIALE TORINO

Alcune notizie dal mondo Cyber… lo sapevate che….



UNIONE INDUSTRIALE TORINO

Alcune notizie dal mondo Cyber… lo sapevate che….



UNIONE INDUSTRIALE TORINO

Alcune notizie dal mondo cyber… lo sapevate che… ci hanno attaccato..

QUANTI HANNO CAMBIATO LA PASSWORD DOPO L'ATTACCO??

(Per gli associati non era fortunatamente necessario, perché abbiamo immediatamente bloccato tutti gli account e forzato il cambio.. ma..)

L'80% delle persone usa la stessa password per tutto!!

PS.. il server era aggiornato…

UNIONE INDUSTRIALE TORINO

Consigli pratici per ridurre il rischio di Hackeraggio delle password..

- **La password della E-mail DEVE essere sempre diversa da tutte le altre** (su ci bucano la password della posta ad esempio, sarà un attimo ricavare le altre di tutti i nostri account social con il «recupera password»)
- Le password vanno «rese semplici» a noi per poterle ricordare sempre:

UNIONE INDUSTRIALE TORINO

Consigli pratici per ridurre il rischio di Hackeraggio delle password.. Concetto di PassPhrase

Ad esempio:

almiosegnalescatenatelinferno

Dividiamo in 3 parti... e al posto delle «a» mettiamo le «@» al posto delle «i» mettiamo «1» al posto delle «l» mettiamo «!» e al posto delle «o» mettiamo lo «0» la prima lettera la mettiamo maiuscola

A!m10segn@ !Esc@ten@t E!1nfern0

UNIONE INDUSTRIALE TORINO

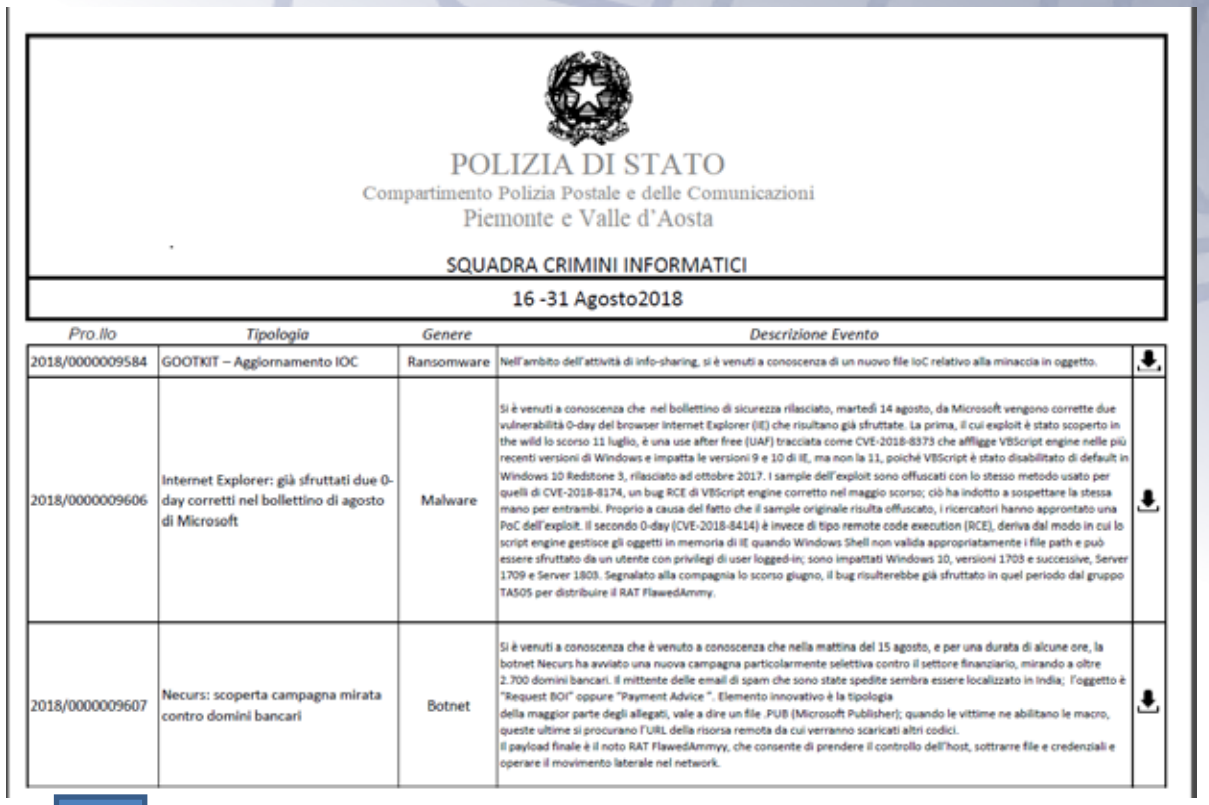
Newsletter «UICONTRAST»

- Da oggi è attivo l'indirizzo mail uicontrast@ui.torino.it che dà origine alla omonima newsletter al quale automaticamente è stato iscritto ogni partecipante al Convegno (con possibilità di disiscrizione dalla prima ricezione..).
- Ad ogni security alerts ricevuto (circa 1-2 ogni mese) verrà inviata agli iscritti copia delle segnalazioni.
- A questo indirizzo è possibile scrivere per ricevere informazioni sulle modalità di presentazione di una segnalazione e di una denuncia in caso di Cybercrimine.

UNIONE INDUSTRIALE TORINO

Come è costruito un report

IOC Pegasus	Cartella di file		
IOC PowerPool	Cartella di file		
IOC Purple Fox	Cartella di file		
IOC Sustes	Cartella di file		
ioc Unsirf Seguito	Cartella di file		
IOC Virobot	Cartella di file		
IOC VPNFilter	Cartella di file		
Nokki	Cartella di file		
Torii	Cartella di file		
Trickbot IOC	Cartella di file		
URSNIF	Cartella di file		
XBash	Cartella di file		
Segnalazioni 2018 Settembre 2.pdf	Documento Adobe Acrobat	413 KB	Sì



POLIZIA DI STATO
Compartimento Polizia Postale e delle Comunicazioni
Piemonte e Valle d'Aosta

SQUADRA CRIMINI INFORMATICI

16 -31 Agosto2018

Pro.llo	*Tipologia*	*Genere*	*Descrizione Evento*
2018/0000009584	GOOTKIT – Aggiornamento IOC	Ransomware	Nell'ambito dell'attività di info-sharing, si è venuti a conoscenza di un nuovo file IoC relativo alla minaccia in oggetto.
2018/0000009606	Internet Explorer: già sfruttati due 0-day corretti nel bollettino di agosto di Microsoft	Malware	Si è venuti a conoscenza che nel bollettino di sicurezza rilasciato, martedì 14 agosto, da Microsoft vengono corrette due vulnerabilità 0-day del browser Internet Explorer (IE) che risultano già sfruttate. La prima, il cui exploit è stato scoperto in the wild lo scorso 11 luglio, è una use after free (UAF) tracciata come CVE-2018-8373 che affligge VBScript engine nelle più recenti versioni di Windows e impatta le versioni 9 e 10 di IE, ma non la 11, poiché VBScript è stato disabilitato di default in Windows 10 Redstone 3, rilasciato ad ottobre 2017. I sample dell'exploit sono offuscati con lo stesso metodo usato per quelli di CVE-2018-8174, un bug RCE di VBScript engine corretto nel maggio scorso; ciò ha indotto a sospettare la stessa mano per entrambi. Proprio a causa del fatto che il sample originale risulta offuscato, i ricercatori hanno approntato una PoC dell'exploit. Il secondo 0-day (CVE-2018-8414) è invece di tipo remote code execution (RCE), deriva dal modo in cui lo script engine gestisce gli oggetti in memoria di IE quando Windows Shell non valida appropriatamente i file path e può essere sfruttato da un utente con privilegi di user logged-in; sono impattati Windows 10, versioni 1703 e successive, Server 1709 e Server 1803. Segnalato alla compagnia lo scorso giugno, il bug risulterebbe già sfruttato in quel periodo dal gruppo TA505 per distribuire il RAT FlawedAmmyy.
2018/0000009607	Necurs: scoperta campagna mirata contro domini bancari	Botnet	Si è venuti a conoscenza che è venuto a conoscenza che nella mattina del 15 agosto, e per una durata di alcune ore, la botnet Necurs ha avviato una nuova campagna particolarmente selettiva contro il settore finanziario, mirando a oltre 2.700 domini bancari. Il mittente delle email di spam che sono state spedite sembra essere localizzato in India; l'oggetto è "Request BOI" oppure "Payment Advice ". Elemento innovativo è la tipologia della maggior parte degli allegati, vale a dire un file .PUB (Microsoft Publisher); quando le vittime ne abilitano le macro, queste ultime si procurano l'URL della risorsa remota da cui verranno scaricati altri codici. Il payload finale è il noto RAT FlawedAmmyy, che consente di prendere il controllo dell'host, sottrarre file e credenziali e operare il movimento laterale nel network.

È un report estremamente TECNICO!!

2018/0000009609	TrickBot: tracciata variante del trojan bancario	Trojan	Si è venuti a conoscenza che Il trojan bancario TrickBot è tornato recentemente alla carica con una nuova variante che si avvale di una tecnica di code injection particolarmente aggressiva. Il malware grazie ad essa può usare call di sistema dirette, avvalersi di tecniche anti-analisi e disabilitare il tool per la sicurezza Windows Defender. La distribuzione avviene grazie a documenti Word malevoli che richiedono l'abilitazione delle macro e inducono le vittime ad avvalersi dello zoom (quest'ultima azione potrebbe essere utile per eludere le sandobox). Una volta eseguito, il malware rimane inerte per 30 secondi grazie alla call Sleep(30000), poi decripta la propria risorsa utilizzando RSA.

UNIONE INDUSTRIALE TORINO

Come utilizzare un report e verificare se è necessario segnalare al Garante il data Breach

Codice	Tipologia	Genere	Descrizione Evento
2018/0000012446	Agent Tesla: attaccanti distribuiscono la minaccia alterando un noto exploit	Trojan	Ricercatori di sicurezza hanno recentemente scoperto una nuova campagna che distribuisce il trojan infostealer legittimo Agent Tesla e altre minacce tra cui Loki. Per diffondere le minacce, gli attaccanti utilizzano una catena d'infezione più volte osservata ma modificata in modo tale da bypassare i controlli dei prodotti di sicurezza. In alcuni casi, l'infezione avviene sfruttando la nota vulnerabilità RCE di Office CVE-2017-0199 per scaricare ed aprire un documento RTF a partire da un file DOCX. In altri casi invece è stato scelto di sfruttare un altro noto bug di Office, CVE-2017-11882 (Equation Editor), per distribuire non solo Tesla e Loki ma anche altre famiglie di malware come Gamarue, che ha la capacità di prendere il completo controllo della macchina target. Da notare però che l'exploit per quest'ultima vulnerabilità è stato leggermente modificato dagli attaccanti in modo da non renderlo riconoscibile per i prodotti di sicurezza; non è chiaro se il codice sia stato manomesso manualmente o se sia stato utilizzato un tool per produrre la shellcode ma di sicuro il metodo è risultato efficace nella campagna in questione e potrebbe essere adottato in altre operazioni di distribuzione malware. Agent Tesla, che viene venduto come tool per il recupero di password e per il child monitoring, è molto sofisticato ed è in grado di rubare credenziali di login da numerosi browser e client di posta tra cui Chrome, Firefox, Opera, Explorer, Outlook, Thunderbird e via dicendo. Può inoltre catturare screenshot, fungere da keylogger, usare la telecamera e consentire l'installazione di ulteriori malware sul sistema infetto (ha infatti anche funzionalità di RAT).
2018/0000013262	CoinTicker: l'applicazione distribuisce le due backdoor EvilOSX e EggShell	Malware	Nei giorni scorsi è stata rilevata un'applicazione chiamata CoinTicker che si spaccia per una legittima utility per il monitoraggio delle criptovalute e che in realtà distribuisce due minacce per sistemi macOS. Nello specifico, si tratta di versioni customizzate delle due backdoor EvilOSX e EggShell, entrambe implementate open-source; una delle modifiche al codice di EvilOSX è stata apportata dall'utente di Github Marten4n6. Da notare nel comportamento di questo malware che non richiede privilegi di root per agire e che risulta efficace anche con i permessi di un utente normale. Al momento non sono noti né il vettore di distribuzione, né l'obiettivo degli attaccanti. Sebbene vi sia una possibilità che le vittime siano state indotte a scaricare CoinTicker da un sito legittimo compromesso, gli analisti sono più confidenti riguardo all'ipotesi che l'APK sia stato realizzato a fini malevoli tout court, poiché l'host dal quale esso viene scaricato è stato registrato solo il 13 luglio scorso. Quanto alle finalità, è probabile che si tenti di avere accesso ai wallet di moneta elettronica per sottrarne il contenuto.

SI

NO

UNIONE INDUSTRIALE TORINO

In caso di avvenuto attacco cosa fare

- Scrivere una mail a uicontrast@ui.torino.it segnalando di voler denunciare l'avvenuto attacco o tentativo di attacco alla Polizia Postale, non è necessario specificare nulla all'UI Torino (**NON INVIARE EMAIL SOSPETTE o EMAIL CONTENENTI VIRUS PER FARSI DARE UN PARERE!!**)
- È possibile fare denuncia in qualsiasi commissariato di Polizia, ma, essendo le nostre aziende principalmente nella Provincia di Torino, ci si può rivolgere direttamente al Compartimento di Polizia Postale (a Torino in Corso Tazzoli 235) per avere una assistenza più dedicata.

È importante avere i dati tecnici corretti per poter fare una denuncia efficace!!

NB: come già detto… se si deve fare segnalazione al Garante farla entro 72 ore da quando ci si è accorti del Data Breach

UNIONE INDUSTRIALE TORINO

Riferimenti:

UFFICIO INFORMATICO UI TORINO:

- Email: p.buttigliengo@ui.torino.it
- Tel. 011.5718.457/313
- Linkedin: paolo-buttigliengo

PEC POLIZIA DI STATO PER REATI INFORMATICI:

compartimento.polposta.to@pecps.poliziadistato.it