Security Awareness

Mercoledì, 14 aprile 2021

AMBITO	FILE .pdf VISUALIZZABILE / SCARICABILE	DATA COMUNICAZIONE DI AWARENESS	DESTINATARI	DESCRIZIONE
Ransomware	CSIRT MI - Alert PYSA-CONTI.pdf (/iam-areariservata-web/documents/20182/1981216/CSIRT+MI+-+Alert+PYSA-CONTI.pdf/3f4cca85-1e05-eee0-7b0f-43dd207666cd?t=1618395041612)	14/04/2021	Dirigenti Scolastici, Direttori dei Servizi Generali e Amministrativi, Istituti Scolastici di ogni ordine e grado	Attacchi informatici della tipologia 'Ransomware' che stanno interessando enti ed organizzazione del settore education. Tale scenario di minaccia cyber si sta ora propagando in Europa dopo essersi manifestato inizialmente in USA ed UK a partire dal marzo 2021, e potrebbe quindi attenzionare anche i sistemi informatici delle varie organizzazioni del settore education italiano, quali istituti scolastici ed università. Nel caso in cui tali attacchi andassero a buon fine, il rischio in particolare per le scuole si concretizzerebbe infatti nell'indisponibilità dei servizi per la didattica a distanza, o nella stessa compromissione di strumenti e software utilizzati per la conduzione delle operazioni didattiche ordinarie, come basi dati gestite da dirigenti e segreterie o gli stessi registri elettronici.
Phishing	CSIRT MI - Alert GOZI.pdf (/iam-areariservata-web/documents/20182/1981216/CSIRT+MI+-+Phishing+Alert+GOZI+19.03.2021.pdf/d6095f86-fe30-e581-406b-8ef5c2f7025a?t=1616407103895)	19/03/2021	Tutti gli utenti Ministero, tutte le scuole statali di ogni ordine e grado, docenti comandati	Campagna di phishing volta a colpire utenti italiani tramite la distribuzione via email di un agente malevolo contenuto in un file excel. Qualora aperto, viene avviata una catena d'infezione della macchina dell'utente. Le email malevole per il Ministero dell'Istruzione si presentano principalmente con oggetto: - "BRT S.P.A. - "fatture scadute *****" - "BRT S.P.A. - "sollecito pagamento fatture **********".

CSIRT-MI - Campagna Ursnif.pdf (/iam-areariservata-web/documents/20182/1981216/CSIRT-MI+Campagna+Ursnif.pdf/8e47c4c3-3a90-4471-2e59-63bebccbae69?t=1607006354788)	16/07/2020	Tutti gli utenti Ministero, tutte le scuole statali di ogni ordine e grado, docenti comandati	Campagna di distribuzione del Trojan URSNIF, anche con impatto specifico verso utenze italiane, operata mediante la distribuzione massiva di email di phishing. L'oggetto della mail farebbe riferimento ad un ordine e relativo pagamento e inviterebbe l'utente ad aprire il file excel infetto ed avviare così la catena d'infezione.
CSIRT-MI - Campagna JasperLoader.pdf (/iam-areariservata-web/documents/20182/1981216/CSIRT-MI+-+Campagna+JasperLoader.pdf/ef0c4027-1dd8-06f2-8b09-ef484def8205?t=1596106070632)	19/06/2020	Tutti gli utenti Ministero, tutte le scuole statali di ogni ordine e grado, docenti comandati	Campagna di distribuzione del malware FTCODE, anche con impatto specifico verso utenze italiane, operata mediante la distribuzione massiva di email di phishing da indirizzi PEC precedentemente compromessi, volta ad indurre in errore gli utenti e favorire l'infezione.
CSIRT-MI - Campagna EMOTET 30.12.2020.pdf (/iam-areariservata-web/documents/20182/1981216/CSIRT-MI+-+Campagna+EMOTET.pdf/73ed0376-6962-6674-e8d8-d7897240ed86?t=1596789763439) (AGGIORNAMENTO)	-	-	Campagna di distribuzione del malware EMOTET, anche con impatto specifico verso utenze italiane, operata mediante la distribuzione massiva di email di phishing operate da un'infrastruttura compromessa. Ulteriori componenti dell'infrastruttura riguardano domini compromessi (generalmente word-press) che agiscono da server di Comando e Controllo ed operano il drop dei payload sul sistema vittima, esfiltrano informazioni rubate e convogliano ulteriori malware ed aggiornamenti. Di recente si è osservato l'impiego del sistema di dropping Emotet in modalità Malware-as-a-Service (MaaS), per la distribuzione di diverse tipologie di agenti malevoli sulle macchine infettate.
CSIRT-MI - Campagna Avaddon.pdf (/iam-areariservata-web/documents/20182/1981216/CSIRT-MI+-+Campagna+Avaddon.pdf/ecd829b6-cbe6-03f9-3769-f1ba77bfdfe6?t=1596106070379)	-	-	Campagna di distribuzione del ransomware Avaddon, anche con impatto specifico verso utenze italiane, operata mediante la distribuzione massiva di email di phishing. La mail di phishing generalmente parla di un procedimento penale proveniente dall'ispettorato del Lavoro che riguarda l'azienda del destinatario.
CSIRT-MI - Campagna AgentTesla.pdf (/iam-areariservata-web/documents/20182/1981216/CSIRT-MI+Campagna+Agent+Tesla.pdf/124ecd88-1906-e5bd-198e-4c800b29c51f?t=1607006354506)	-	-	Campagna di distribuzione del malware AgentTesla, operata mediante la distribuzione massiva di email di phishing. L'oggetto delle email è generalmente relativo ad una presunta copia di un pagamento e data di spedizione oppure la stessa mail si presenta come proveniente da una società di consulenza.

Malware	CSIRT-MI - Campagna Dridex.pdf (/iam-areariservata-web/documents/20182/1981216/CSIRT-MI+-+Campagna+Dridex.pdf/64da6f7c-aadc-88a6-fac7-407bc86f5b31?t=1605006672616)	-	-	Campagna di distribuzione del malware Dridex, operata mediante la distribuzione massiva di email di phishing. Sfrutta i riferimenti ad aziende private per ingenerare sicurezza nell'utente vittima, invita il destinatario a prendere visione di una fattura presente nel documento allegato.
	CSIRT-MI - Malware as-a-service BUER.pdf (/iam-areariservata-web/documents/20182/1981216/CSIRT-MI+-+Malware+as-a-service+BUER.pdf/1c648bb6-72cd-b316-6322-15b6d6dadb41?t=1605006672928)	-	-	Malware avente scopo nativo di fornire un primo punto di accesso, compromettendo sistemi operativi basati su Microsoft Windows, per garantire agli attaccanti successive attività malevole. Inizialmente utilizzato in attacchi finalizzati a distribuire malware bancari, Buer, attualmente, viene sfruttato anche negli attacchi ransomware.
	CSIRT-MI - Variante malware ComRAT.pdf (/iam-areariservata-web/documents/20182/1981216/CSIRT-MI+-+Variante+malware+ComRAT.pdf/5f2c54ac-792f-bf5c-50d0-cdb0b1d23fda?t=1605006673226)	-	-	La tecnica impiegata per questo malware prevede l'iniezione di un modulo di comunicazione nel browser di default del sistema target utilizzato per inviare e ricevere richieste e risposte http dai e verso i server di Comando e Controllo dell'attaccante, implementando così un sistema di "backdoor command" (ossia per il controllo da remoto).