ویانا؛ ۲۰۲۰/۰۴/۱۴ مصادف با ۲۹ حمل ۱۳۹۹

جرایم سایبری و کووید-۱۹: خطرات و پاسخ ها

قضاوت های کلیدی

- **جرایم سایبری در پاسخ به بیماری فراگیر کووید-۱۹ ظهور و رشد می نماید.** تقلب آنلاین، اخاذی و آزار و اذیب جنسی اطفال بصورت آنلاین افراد را مورد هدف قرار میدهد، در حالیکه اخاذی سیستماتیک انترنتی یا (Ransomware) معمولاً سیستم ها را – به شمول شفاخانه ها، مورد هدف قرار میدهد. موضوع مورد هدف قرار گرفتن دولت ها از طریق حملات نرم افزار های بد یا (Malware) ادامه خواهد داشت. انتشار رو به افزایش معلومات غلط و دروغ پراگنی ها (شایعه افگنی ها) به هدف مغشوش ساختن اذهان عامه و تضعیف پاسخ علمی، ادامه خواهد داشت.
- **انجام کارهای رسمی از خانه احتمال بیشتر شدن آمار قربانیان جرایم سایبری را افزایش داده است. مردم در خانه ها با خطرات جدی تر آنلاین مواجه اند، چون خود را بگونه غیرعمدی در معرض خطر مجرمین سایبری تکنالوجی معلوماتی، قرار میدهند.** هک کردن سیستم به طریقه (Phishing) به هدف دسترسی های خصمانه مجرمین و سائر فاعلین پیشرفته، به سیستم های مهم ادامه خواهد داشت.
- **کمیت متخصصین پرسونل بخش تنفیذ قانون مبارزه علیه جرایم سایبری در طول سال (۲۰۲۰) کاهش خواهد یافت. جرایم سایبری در زمان محدود افزایش خواهد یافت، و ممکن است قربانیان در راه رسیدن به عدالت با تأخیرات روبرو گردند.** مجرمین سایبری از خلاء های مشهود عملیاتی سود خواهند برد. این کار بگونه غیر منطقی باعث ایجاد فرصت های تکتیکی و ستراتیژیک در بخش تنفیذ قانون خواهد گردید.

خلاصه متن

1. این معلومات مختصر یک تصویر کوچک تهدیدات جرایم سایبری در محدوده بیماری فراگیر کووید-۱۹ را ارائه می نماید. معلومات متذکره از جمع معلومات محرم بخش های تنفیذ قانون، بخش های دولتی، اکادمیک، رسانه ئی، منابع باز و شرکاء سکتور خصوصی دفتر مبارزه علیه جرایم و مواد مخدر سازمان ملل متحد (UNODC) در سرتاسر جهان، در جریان ماه اپریل سال (۲۰۲۰) میلادی، جمع آوری گردیده است. توصیه ها در اخیر شرح هر موضوع، ارائه گردیده اند.

تصویر تهدید: در حال ظهور، افزایش و بهره برداری

2. امروزه اقدامات وسیع فاصله گیری اجتماعی در سرتاسر جهان روی دست گرفته شده اند. این کار به گونه چشمگیری استفاده از مکالمات آنلاین (انترنتی) را در میان کارمندان ادارات، بخش های تجاری و افراد عادی، افزایش داده است. بیشتر افراد متذکره در استفاده از تکنالوجی آنلاین، بلدیت کامل ندارند. این کار باعث ایجاد یک هدف بزرگ، دلچسپ وآسیب پذیر برای مجرمین سایبری گردیده، تا از آن بهره ببرند. بخاطر اینکه کارهای رسمی دفاتر و تدریس نهاد های آموزشی بگونه آنلاین به پیش میروند، آنعده استفاده کننده گان انترنت، که راجع به تهدیدات سایبری کمتر میدانند، بیشتر گردیده و احتمال دارد که در خانه های شان نسبت به ساحه کاری یا مکان آموشی شان، در معرض بیشتر خطرات سایبری قرار داشته باشند.
3. مجرمین سایبری به هدف بهره برداری از تغییرات بوجود آمده اجتماعی، حقوقی و روانی ناشی از کووید-۱۹، فعالیت های جرمی شانرا انجام می دهند. اطفال مکتب رو، خواه استفاده کننده گان جدید یا قبلی انترنت باشند، بگونه پیشگیرانه مورد هدف مجرمین جنسی آنلاین قرار میگیرند. این ها شامل مجرمین با هدف آموزش یا (Groom[1]) و آسیب جنسی یا

[1] https://www.esafety.gov.au/parents/big-issues/unwanted-contact

(Sextort[2]) تا به دسترسی گسترده تر به هریکی از اطفال در صنوف آنلاین[3] که حالا بنام بمباران زوم یا "Zoom-Bombing" یاد میشوند، میگردند.

4. مجرمین با استفاده از ترس مردم راجع به وایرس کووید-۱۹: با پیشکش نمودن راه های معالجه فروشی در انترنت و فریب دادن مردم از طریق فروش مواد ضدعفونی کننده دستان و تجهیزات محافظتی شخصی، دارو ها یا مواد حفظ الصحی که اصلاً وجود ندارند، بصورت گسترده صید می نماید. سائر فریب ها شامل پیشکش خدمات، مانند؛ مشوره دهی راجع به سرمایه گذاری نادرست (به شمول ارز های دیجیتلی یا Cryptocurrencies) و مشوره دهی و تشخیص غلط طبی، میگردند. یکی از سایت های انترنتی غیراخلاقی به کاربران اش در یکی از کشورها اجازه اشتراک رایگان را داده است، که این کار خطرات دانلود نرم افزارهای بد یا (Malware) و آسیب جنسی یا (Sextortion) را افزایش داده است.

5. شهروان بزرگ سال که اغلباً در مقابل خطرات آنلاین کمتر حساس هستند، بگونه واضح و نمایان، با دانلود و فرستادن لینک های ملوث با نرم افزار بد انترنتی یا (Ransomware) از طریق ایمیل های سپم مرتبط به کووید-۱۹ مورد هدف مجرمین سایبری قرار میگیرند، و معلومات دروغ را با دوستان و فامیل شان شریک میسازند. مجرمین سایبری با ادعا نمودن اینکه راجع به استفاده غیراخلاقی آنلاین به اصطلاح قربانی خویش میدانند – و آنرا فاش خواهند نمود، به اخاذی ادامه میدهند.

6. در اختیار گرفتن[4] ایمیل تجاری (هک کردن به طریقه Phishing – حساب های ایمیل ظاهراً یک مسؤول بلند رتبه در نهاد مورد هدف را در اختیار میگیرند) به هدف استفاده از انجنیری – اجتماعی، که توأم با تعجیل مرتبط به این مرض فراگیر میباشد، در راستای انتقال پول ها به یک بانک جرمی، مبادله پول ها به ارز خارجی یا حساب ارز های دیجیتلی (Cryptocurrencies)، و یا هم به هدف بدست آوردن دیتای حساس برای استفاده خصمانه، به شمول جاسوسی، ادامه خواهد داشت.

7. بازار انترنت سیاه (جرمی) به فروش دیتای جمع آوری شده غیرقانونی – به شمول دیتای مرتبط به افراد بلند پایه و چهره های مشهور، ادامه می دهد. مجرمین که تازه به "جرم سایبری" روی آورده اند، راجع به چگونگی بهترین وجه بهره برداری از مرض فراگیر کووید-۱۹ به هدف بدست آوردن منفعت، از مجرمین دیگر رهنمائی دریافت می نمایند. بعضی از مجرمین سایبری، دیگر مجرمین سایبری را از مورد هدف قراردادن شفاخانه ها و لابراتوارهای آزمایش واکسین از طریق حملات انکار گسترده خدمات یا (DDOS) و اخاذی سیستماتیک انترنتی یا (Ransomware)، منصرف نموده اند. مجرمین درنده جرایم جنسی اطفال راجع به اینکه کدام شبکه اجتماعی یا سایت های تشریک عکس ها به آنان فرصت میدهد تا به آسانی به سوء استفاده از اطفال بپردازند، بحث میکنند. مجرمین در مورد چگونگی بهترین شیوه تشخیص و شکست دادن پولیس های مخفی آنلاین نیز، بحث و تبادل نظر می نمایند.

8. بر علاوه مجرمین سایبری عادی، گروه های خطرمداوم پیشرفته یا (APT) نیز به گسترش و بهره برداری از این مرض فراگیر، ادامه می دهند. خطرات مداوم پیشرفته یا (APTs) به مورد هدف قرار دادن زیربناهای مهم ملی، به شمول شفاخانه ها و لابراتوارهای ساخت واکسین، از طریق حملات (Malware)، (Ransomware) و (DDOS) ادامه میدهند. انگیزه چنین حملات تنها موضوع دریافت منفعت مادی نیست، بلکه (Malware) معمولاً دسترسی به اختیارات وردی یا (Login) و سائر معلومات حساس با ارزش استخباراتی را، فراهم می سازد.

9. موفقیت بیشتر جرایم سایبری مرتبط به کووید-۱۹، وابسته به حملات هک کردن ایمیل یا (Email Phishing) میگردد، چون ایمیل مسیر اساسی دسترسی به معلومات را فراهم می نماید. زمانیکه مردم بالای یک لینک یا سند کلک می نمایند، حساب شان به کنترول مجرمین قرار میگیرد. این دسترسی به کنترول حساب کاربری ممکن است به خود قربانی قابل مشاهده باشد، اما در اغلب موارد پنهان می ماند تا به مجرمین فرصت ایجاد و تحکیم دسترسی طویل المدت به حساب کاربری، نهاد یا مرکز تکنالوجی معلوماتی مربوطه را، فراهم نماید. بر علاوه جمع آوری معلومات حساس، عامل خطرمداوم پیشرفته یا (APT) میتواند ویبسایت ها را بد شکل سازند، جزئیات اسناد را تغییر دهد، دیتا را حذف نمایند و معلومات غلط و دروغ را نشر و پخش نمایند.

10. **دفتر مبارزه علیه جرایم و مواد مخدر سازمان ملل متحد (UNODC) به دولت ها و سکتور خصوصی توصیه می نماید تا کمپاین های آگاهی دهی عامه را طوری افزایش دهند که دربرگیرنده موضوعات حساس کلتوری بوده و به آسانی قابل فهم باشند. مراکز راپوردهی سوء استفاده جنسی از اطفال (hotlines) بصورت گمنام، یک شیوه کلیدی مجادله با**

[2] https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion
[3] https://tcrn.ch/3buz3gW
[4] https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

آن میباشد. ما همچنان توصیه می نمائیم که رهنمای های جدید امنیتی بگونه جدی عملی گردیده، معلومات به روال عادی، ذخیره احتیاطی یا (Back-Up) گردند.

کاهش ظرفیت بخش تنفیذ قانون و انعطاف پذیری اجتماعی

11. در بسیاری از کشورهای جهان، پرسونل متخصص مبارزه علیه جرایم سایبری از بخش تحقیق جرایم سایبری، به بخش اقدامات حمایوی دولت، مانند؛ تنفیذ قرنطین علیه شیوع کووید-۱۹، انتقال گردیده اند. مسؤولین متخصص بیمار نیز گردیده اند. انتظار میرود که در هفته های آینده ظرفیت کاهش یابد، و این کار باعث کاهش توانائی دولت ها در امر مبارزه علیه تهدیدات جرایم رو به افزایش و جدید سایبری، خواهد شد.

12. در چندین کشور جهان، روند تحقیقی و قضائی از هم گسیخته اند، و نیاز است تا فعالیت های متذکره توسط خود شخص انجام شوند، چیزیکه بنابر اقدامات صحی هرکشور، غیرممکن میباشد. کشورهای دیگر سریعاً به فعالیت های قضائی آنلاین روآورده اند.

13. معلومات غلط و دروغ پراگنی ها (شایعه افگنی ها) راجع به وایرس متذکره، عمدتاً از طریق رسانه های اجتماعی و خدمات پیام رسانی پنهانی، رو به گسترش میباشد. کمپنی های رسانه های اجتماعی نیز بخاطر انجام کارها از راه دور، با چالش مواجه اند، و سعی میورزند تا با کمیت معلومات غلط مجادله نموده، پالیسی های داخلی و فشار های قوانین مربوطه را بگونه درست عملی نمایند.

14. معلومات غلط، دروغ پراگنی ها (شایعه افگنی ها) و حملات بالای زیربناهای مهم ملی باعث تخریب اعتماد عامه گردیده و اثرگذاری اقدامات مصؤونیت عامه را تضعیف می نماید.

15. **دفتر مبارزه علیه جرایم و مواد مخدر سازمان ملل متحد (UNODC) توصیه می نماید تا در صورت امکان، و حصول اطمینان راجع به حفظ معیارات و نورم های بین المللی، حقوق اولیه شهروندان و حاکمیت قانون، روند های قضائی بگونه آنلاین ادامه یابند.**

16. **ما همچنان توصیه می نمائیم که کمپنی های شبکه های اجتماعی در قسمت مبارزه علیه گسترش معلومات غلط مرتبط به مرض فراگیر کووید-۱۹ یا "Misinfodemic"، با حفظ آزادی بیان، سعی بیشتر نمایند. معلومات عملی مبتنی بر حقایق باید در قلب پاسخ کووید-۱۹ قرار گیرد – همه ای مان یک نقش کلیدی در این کار داریم.**

تحلیل و تجزیه

a. *مرض فراگیر کووید-۱۹ باعث یک چالش بی سابقه جهانی به تمام جوامع گردیده است. بسیاری از جوامع فعالیت های شانرا بصورت آنلاین تغیر داده اند، مجرمین نیز چنین کرده اند. در حالیکه جرایم سایبری بصورت پیچیده و قربانیان از نظر کمیت افزایش میابند، در بعضی از کشورها مسؤولین بخش تنفیذ قانون به وظایف دیگر گماشته میشوند. تاثیرات اقتصادی کووید-۱۹ یک لایهء دیگری به پیچیده گی ها برای مردم و دولت، اضافه نموده است. یک طوفان احتمالی جرایم سایبری در حال ظهور میباشد.*

b. *در حالیکه کووید-۱۹ و تهدیدات جرایم سایبری مرتبط به بحران متذکره جهانی اند، پاسخ ها نیز باید جهانی باشند: مبارزه علیه جرایم سایبری در یکی از حوزه های قضائی، خطر آنرا در سرتاسر جهان کاهش میدهد. معلومات مرتبط به تهدیدات جدید و انواع تازه جرایم سایبری، مانند؛ تحلیل کووید-۱۹ پولیس اروپا یا (Europol's COVID19 analysis) و ارزیابی تهدید سایبری پولیس بین المللی یا (INTERPOL's Cyber Threat Assessment) باید بدون وقفه، بصورت بین المللی شریک ساخته شوند. مراکز راپوردهی سوء استفاده جنسی از اطفال (hotlines)، یک وسیله مهم در راستای توانمندسازی مردم عام در امر مبارزه با آن میباشد.*

c. *با درنظرداشت فشار بالای هردو بخش کنشی و واکنشی تنفیذ قانون، ارزیابی مان نشان میدهد که ظرفیت تحقیق فعالانه جرایم سایبری در کوتاه – مدت با چالش روبرو خواهد شد – مخصوصاً در کشورهایکه قبل از این مرض فراگیر، دارای منابع محدود بوده اند. مجرمین سایبری، به شمول گروه های (APT) به بهره گیری شان از این معضله ادامه خواهند داد. راپور دهی مردم عام که سبب دستگیری مؤفقانه یا مختل سازی فعالیت های آنعده مجرمین سایبری میگردد که از حالت بوجود آمده نفع میبرند، باید تقویت گردد. عملیات های خیلی کوبنده، مانند؛ از کار انداختن پنجاه تهیه کننده گان (DDoS)*

در یک هفته[5] در نیدرلند (هالند) کمک می نماید تا به مجرمین سایبری گوشزد گردد که عملیات ها علیه آنان در سرتاسر جهان ادمه خواهند یافت. عملیات های مخفی کنشی آنلاین علیه عاملین خطرات بلند جرایم سایبری، باید ادامه یابد. برخلاف اصل موضوع، ممکن است مجرمین به پذیرش خطرات بیشتر بگونه آنلاین موافقت نمایند، چون حدس میزنند که احتمال کشف آنان کاهش یافته است. بناً؛ تحقیقات متخصصین بخش تنفیذ قانون باید به سرعت ادامه یابند.

d. سیاست عامه و بلندبردن آگاهی موضوعات مهم در راستای جلوگیری میباشند، و باید گروه های آسیب پذیر، مانند؛ اطفال و بزرگ سالان را، تقویت نماید. اقدامات علیه معلومات غلط و دروغ پراگنی ها (شایعه افگنی ها) باید منجر به معلومات ارزیابی شده، قابل اعتماد و مفید گردند. این کار باید به یک طریقه شفاف و قابل محاسبه انجام شود.

e. تمام اقدامات مرتبط به مبارزه علیه جرایم سایبری باید متناسب، حقوقی، قابل محاسبه و لازمی باشند. بسیاری از کشورها با استفاده از تکنالوجی، مریضان کووید-۱۹ را ارزیابی، تشخیص و پیگیری می نمایند. این کار مهم باید با یک نظارت شفاف به هدف اطمینان از اینکه اقدامات مراقبتی متذکره بعد از بدست آمدن هدف – که همانا کنترول شیوع است، خاتمه می یابد، تحت بررسی قرار داشته باشد. حالا وقت آن رسیده تا بصورت عام اطمینان – سایبری حاصل نموده، باهم کار کنیم تا با بیشترین تهدیدات ناخوشایند زمانه خویش مبارزه نموده، اطمینان را به سطح جهانی (بین المللی) احیاء نمائیم.

f. حالا وقت آن نیست که سرمایه گذاری مان در بخش تخصصی جرایم سایبری تنفیذ قانون بیجا باشد. توانائی و ظرفیت مبارزه علیه جرایم سایبری بخش های مهم حفاظت از زیربناهای مهم ملی، مصؤون نگهداری اطفال بگونه آنلاین، تقویت بخش صنعتی، محافظت شفاخانه ها و همکاری در احیاء ای اقتصادی بعد از کووید۱۹ ، میباشند.

g. کارمندان متخصص بخش جرایم سایبری دفتر مبارزه علیه جرایم و مواد مخدر سازمان ملل متحد (UNODC) در سرتاسر جهان، برای همکاری با کشورهای عضوء در امر مبارزه علیه جرایم سایبری، بطور (۲۴) ساعته، هفت (۷) روز در هفته، قابل دسترس اند. منابع سیاست عامه دفتر مبارزه علیه جرایم و مواد مخدر سازمان ملل متحد (UNODC) در این لینک: https://www.unodc.org/unodc/en/covid-19.html ، و لینک های پخش زنده مصاحبه انستاگرام: Instagram Live با سکرتر جنرال فرستاده ویژه برای جوانان، توصیه های محافظتی برای کارمندان سازمان ملل متحد: UN staff و بخش وسیع سایبری مرتبط به سکرتریت سازمان ملل متحد: iSEEK Live قابل دسترس اند.

انتشار: شما میتوانید این راپور (UNODC/CMLS/COVID19/Cyber1) را بدون اخذ اجازه قبلی از تهیه کننده آن، نشر نمائید.

خاتمه

[5] https://www.zdnet.com/article/dutch-police-take-down-15-ddos-services-in-a-week/