****

**Մամուլի հաղորդագրություն**

**«Կասպերսկի Լաբորատորիա»-ն կանխատեսել է 2019-ին կիբեռսպառնալիքների զարգացման հիմնական միտումները**

**Երևան, 24 դեկտեմբերի, «Կասպերսկի Լաբորատորիա»-ի Հայաստանի ներկայացուցչություն։**  «Կասպերսկի Լաբորատորիա»-ի փորձագետները, ամփոփելով անցնող տարվա ընթացքում կիբեռճակատում դիմակայության արդյունքները, [առանձնացրել են](https://securelist.ru/kaspersky-security-bulletin-threat-predictions-for-2019/92782/) միտումներ, որոնք, մեծ հավանականությամբ, կպահպանեն արդիականությունը մոտ ապագայում։

Ինչպես և նախկինում, առավել լուրջ վտանգ կկրեն [APT-արշավները](https://encyclopedia.kaspersky.ru/glossary/apt-advanced-persistent-threats/?utm_source=threatpost&utm_medium=blog&utm_campaign=termin-explanation). դրանք բարդ են, դժվար հայտնաբերվող, իսկ այդ գրոհների իրականացման ժամանակ օգտագործվող գործիքակազմն անընդհատ կատարելագործվում է։ Դրա հետ մեկտեղ, նպատակին հասնելու համար լավ ֆինանսավորվող չարագործները երբեմն մեծացնում են ընդգրկումը. գրոհում են ծառայությունների մատակարարներին կամ ենթակառուցվածքը, որն այդ նպատակակետն օգտագործում է։ APT-ի շրջանակում որոշ գործողություններ իրականացնում են վարձկանները՝ իրենց գործիքներով և տեխնիկաներով, ինչն էապես դժվարացնում է հատկորոշումը։

Ինչ վերաբերում է ենթակառուցվածքի վրա ազդեցությանը, ապա փորձագետները ենթադրում են, որ կարելի է սպասել այնպիսի բազային տարրերի վրա գրոհների հաճախակիացմանը, ինչպիսին են ցանցային սարքերը։ Դրանց հիմքի վրա կարելի է կառուցել բոտերի ունիվերսալ ցանց (դրա վառ օրինակն է [VPNFilter](https://threatpost.ru/fbi-seizing-vpnfilter-c2-domain/26244/)-ը) և այն օգտագործել, ի թիվս այլոց, քիչ նկատելի թիրախային գրոհների իրականացման համար։ Առանձնակի տագնապ է առաջացնում IoT-բոտնետերի բանակի աճը. հմուտ ձեռքերում դրանք ի զորու են վերածվել կրիտիկական կարևոր օբյեկտներն արդյունավետ շարքից հանելու գործիքի։

 [Olympic Destroyer](https://threatpost.ru/wiper-attacked-olympic-games-2018-servers/24593/)-ի նման դեստրուկտիվ գրոհները վաղ է հաշվից դուրս գցել, թեև դրանք մինչ այժմ քիչ են տարածված։ Նման ակցիաները հաճախ կատարում են ծխաշղարշի դեր, սակայն կարող են օգտագործվել «որպես վրեժի գործիք, որը միջանկյալ դիրք է զբաղեցնում դիվանագիտական պատասխանի և ռազմական գործողությունների միջև»։

APT-արշավների ընթացքում վարակման ամենագործուն վեկտոր է եղել և մնում [թիրախային ֆիշինգը](https://encyclopedia.kaspersky.ru/glossary/spear-phishing/?utm_source=threatpost&utm_medium=blog&utm_campaign=termin-explanation)։ Այդ մոտեցումը չարագործներին օգնում են կատարելագործել ոչ միայն հետախուզության ավանդական մեթոդները, այլև սոցցանցերից արտահոսքերը։ Վերջիններս, ցավոք, տեղի են ունենում ավելի հաճախ և նախկինի համեմատ մեծ ծավալով, բավարար է հիշել [Facebook](https://threatpost.ru/facebook-admits-potential-breach-of-90-mln-users-data/28483/)-ի աղմկահարույց դեպքը։ 2018-ին դիտարկվել են նաև ֆիշինգի արդյունավետությունը մեքենայական ուսուցման օգնությամբ մեծացնելու փորձեր։

**Ֆինանսական հատված**

Փորձագետները ցավով [արձանագրում են](https://securelist.ru/ksb-cyberthreats-to-financial-institutions-2019-overview-and-predictions/92852/), որ այդ ճակատում գործող ամենախոշոր [Carbanak/Cobalt](https://threatpost.ru/head-of-cobalt-gang-arrested-in-spain/25278/) և [Fin7](https://threatpost.ru/three-ukrainians-arrested-for-cybercrime/27548/) խմբերի անդամների ձերբակալությունը չի հանգեցրել դրանց գործողությունների դադարեցմանը։ Քրեական հանրույթները սկսել են մասնատվել, արդյունքում՝ գրոհները հաճախակիացել են, իսկ հնարավոր զոհերի աշխարհագրությունը՝ ընդլայնվել։ Նոր խմբավորումների ակտիվության աճը հատկապես նկատելի է Հնդկա-Պակիստանյան տարածաշրջանում, Հարավ-Արևելյան Ասիայում և Կենտրոնական Եվրոպայում։ Այդ երկրներում չարագործներին գրավում է «ֆինանսական հատվածում պաշտպանական լուծումների ոչ հասուն լինելը»՝ էլեկտրոնային վճարումների ոլորտի բուռն աճի ֆոնի վրա։

Հետազոտողները նաև դիտարկում են PoS-տերմինալների վրա գրոհների քանակի նվազում։ Չարագործների մի մասն անցել է առցանց-վճարումների ընդունման համակարգերին, քանի որ այդ դեպքում հարձակման արդյունքները ավելի հեշտ է վերածել փողի։ Նման գրոհներն առավել վտանգավոր են առանց չիպերի քարտերի տերերի և առցանց-բանկինգի հաճախորդների համար, որոնք անտեսում են մուտքի երկգործոն ստուգումը։

Նույնականացման կենսաչափական համակարգերի ներդրումն արդեն իր վրա է սևեռել կիբեռհանցագործների ուշադրությունը։ 2018-ին փորձագետները սև շուկայում [հայտնաբերել են](https://threatpost.ru/issledovateli-kibermoshenniki-interesuyutsya-biometriej/18279/) մատնադրոշմներ ճանաչելու համակարգեր և սքիմերներ, որոնք ի զորու են ստանալ կենսաչափական տվյալները։ Գրանցվել է նաև նման տեղեկատվության մի քանի [խոշոր](https://threatpost.ru/opm-hack-expands-to-include-data-of-21-5-million-people/9785/) [արտահոսք](https://threatpost.ru/micro-market-vendor-warns-of-bankcard-and-biometric-data-breach/21875/)։

Ֆինանսիստների համար ծրագրային ապահովման մատակարարների վրա գրոհներն ապացուցել են իրենց արդյունավետությունը և, ըստ երևույթին, կշարունակվեն նաև առաջիկայում։ Հարկ է նաև նոր գործողություններ սպասել [ВЕС-չարագործների](https://encyclopedia.kaspersky.ru/glossary/bec/?utm_source=threatpost&utm_medium=blog&utm_campaign=termin-explanation) կողմից. նրանք հմտացել են այն տվյալների ձեռքբերման գործում, որոնք անհրաժեշտ են ընկերությունների միջոցների փոխանցման համար պատասխանատու աշխատակիցներին հաջող խաբելու համար։

Բանկի ներքին ցանցին միացող [հեռավար հասանելիությամբ սարքերը](https://securelist.ru/darkvishnya/92908/) ներգրավելու միտումը նույնպես, ըստ ամենայնի, կպահպանվի։ Օգտվելով կազմակերպություններում ֆիզիկական անվտանգության նկատմամբ անփույթ վերաբերմունքից և միացվող սարքերի նկատմամբ հսկողության բացակայությունից, չարագործները շենքում թաքուն տեղադրում են նեթբուք կամ մինի-պլատա, որպեսզի ձեռք գցեն տվյալները ներկառուցված GPRS/3G/LTE-մոդեմի օգնությամբ՝ այդպես ստանալով տեղեկատվություն հաճախորդների և ցանցային ենթակառուցվածքի մասին։

Մոբայլ բանկինգի համակարգերի օգտատերերի համար հեռանկարներն անուրախ են մնում։ Տարվա ընթացքում «Կասպերսկի Լաբորատորիա»-ում գրանցել են 144 հազ. մասնագիտացված վնասաբեր ծրագրեր, և այդ բանակն, ըստ դիտարկումների, բազմապատկվում է։ Ավելին՝ բիզնեսի համար մոբայլ հավելվածների ժողովրդականության աճն անխուսափելիորեն կբերի դրանց օգտատերերի վրա գրոհների, քանի որ կազմակերպությունների հաշիվներին հասանելիությունը խոստանում է ավելի մեծ օգուտ, քան ֆիզիկական անձանց դեպքում։ Փորձագետների սպասումներով՝ այդ նպատակով իրավաբանական անձանց վրա գրոհները կիրականցվեն, ամենից հավանական է, վեբ-API-ի և մատակարարումների շղթայի միջոցով։

**Արդյունաբերական արտադրություն**

Այս ոլորտում գրոհները [համեմատաբար հազվադեպ են](https://securelist.ru/ksb-threat-predictions-for-industrial-security-in-2019/92848/). դրանք ավելի բարդ է փողի վերածել, իսկ շուկայում առկա գործիքները և մարտավարությունները հարմարեցում են պահանջում։ Այդուհանդերձ, ավտոմատացման միջոցների ժողովրդականության և բազմազանության աճը, ինչպես նաև նման համակարգերը հեռավար օգտագործելու ընդհանուր ձգտումն ընդլայնում են [գրոհի մակերեսը](https://encyclopedia.kaspersky.ru/glossary/attack-surface/) հնարավոր չարագործների համար, և դա չի կարող չանհանգստացնել։

Ավտոմատացված կառավարմամբ օբյեկտները՝ հատկապես, ռազմավարական նշանակություն ունեցող, միշտ արժանացել են հատուկ ծառայությունների ավելի մեծ ուշադրությանը։ Այդպիսի ձեռնարկությունների վրա գրոհները կարող են լինել ոչ միայն արդյունաբերական լրտեսության միջոց, այլև երկրի վրա ճնշում գործադրելու գործիք։ Հաշվի առնելով աշխարհաքաղաքական դրությունը՝ փորձագետները ենթադրում են, որ մոտակա տարիներին ճնշման այդ եղանակը կպահպանի արդիականությունը։

Ցավոք, տեխնոլոգիական գործընթացների կառավարման ավտոմատացված համակարգերի (ՏԳ ԿԱՀ) պաշտպանությունը հեռու է բավարար լինելուց։ Լայն հանրությունը տեղեկացված չէ այդ ոլորտում կիբեռանվտանգության հիմնախնդիրների մասին, իսկ կիբեռմիջադեպերի հազվադեպ բախվող կազմակերպությունները դեռևս ապավինում են վթարային պաշտպանության համակարգերին։ Արդյունաբերական ձեռնարկություններին ուղղված հնարավոր սպառնալիքներին դիմակայելու համար ստեղծվող լուծումներն անկատար են, և, փորձագետների կարծիքով, ունակ չեն պաշտպանել իրական գրոհներից։

**Կրիպտոարժույթների շուկա**

«Կասպերսկի Լաբորատորիա»-ի վիճակագրության համաձայն՝ այս տարի մայնինգի համար նախատեսված ծրագրերով վարակման փորձերի քանակն ավելի մեծ է եղել, քան [շորթող ծրագրերինը](https://encyclopedia.kaspersky.ru/glossary/ransomware/?utm_source=threatpost&utm_medium=blog&utm_campaign=termin-explanation)։ Մասնավորապես, 2017 թվականի համեմատ գրեթե կրկնակի [աճել է](https://www.kaspersky.ru/about/press-releases/2018_miners-surpassed-extortionists-kaspersky-lab-summed-up-the-results-of-2018) թաքնված մայնինգի ծրագրերով վարակման փորձերի ենթարկված ռուսաստանցի օգտատերերի թիվը։ Երկրորդ կիսամյակում կրիպտոարժույթների փոխարժեքի անկման պատճառով դրանց նկատմամբ հետաքրքրությունը ճակատի երկու կողմերում նվազեց, սակայն, հետազոտողները կանխատեսում են, որ կրիպտոջեքինգը՝ որպես սպառնալիք, կպահպանի իր արդիականությունը, իսկ մայներների քանակը կշարունակի աճել։

Բուն կրիպտոարժույթները՝ որպես վճարամիջոց, փորձագետների կարծիքով, աստիճանաբար կկորցնեն ժողովրդականությունը՝ չափազանց մեծ կոմիսիոն վճարների, շատ դանդաղ փոխանցման, ինտեգրման մեծ արժեքի և հաճախորդների սահմանափակ թվի պատճառով։ Վերջին գործոնը հատկապես կարևոր է. փոքր պահանջարկն արագ կբավարարվի, և փոխարժեքները կդադարեն մեծանալ։

Ինչ վերաբերում է [բլոկչեյններին](https://encyclopedia.kaspersky.ru/glossary/blockchain/?utm_source=threatpost&utm_medium=blog&utm_campaign=termin-explanation), ապա այդ տեխնոլոգիայի ելքը կրիպտոարժույթների շուկայի սահմաններից դուրս, ինչպես համոզվել են շատերը, իրեն չի արդարացրել։ Ըստ երևույթին, դրա կիրառման ոլորտն այդպես էլ նեղ կմնա. փորձագետները ենթադրում են, որ այդ բնագավառում բոլոր փորձարկումները հետագայում կդադարեն։

*«Կասպերսկի Լաբորատորիա» ընկերության Հայաստանի ներկայացուցչություն*

*Հարցերի համար դիմել +374 10 58 26 20 հեռախոսահամարով*