勒索病毒流行态势分析

2021 年 7 月勒索病毒流行态势分析

360CERT
北京奇虎科技有限公司

报告信息

报告名称	2021 年 7 月勒索病毒流行态势分析		
报告类型	勒索病毒流行态势分析	报告编号	B6-2021-080902
报告版本	1	报告日期	2021-08-09
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-08-09	360CERT	360CERT	撰写报告

目录

1 摘要

勒索病毒威胁仍是当前最热门的网络安全风险，360 反勒索服务已累计接收处置数万勒索病毒感染求助。随着新型勒索病毒的快速蔓延，企业数据泄露风险不断上升，数百万甚至上亿赎金的勒索案件不断出现。勒索病毒给企业和个人带来的影响范围越来越广，危害性也越来越大。360 安全大脑针对勒索病毒进行了全方位的监控与防御，为需要帮助的用户提供 360 反勒索服务。

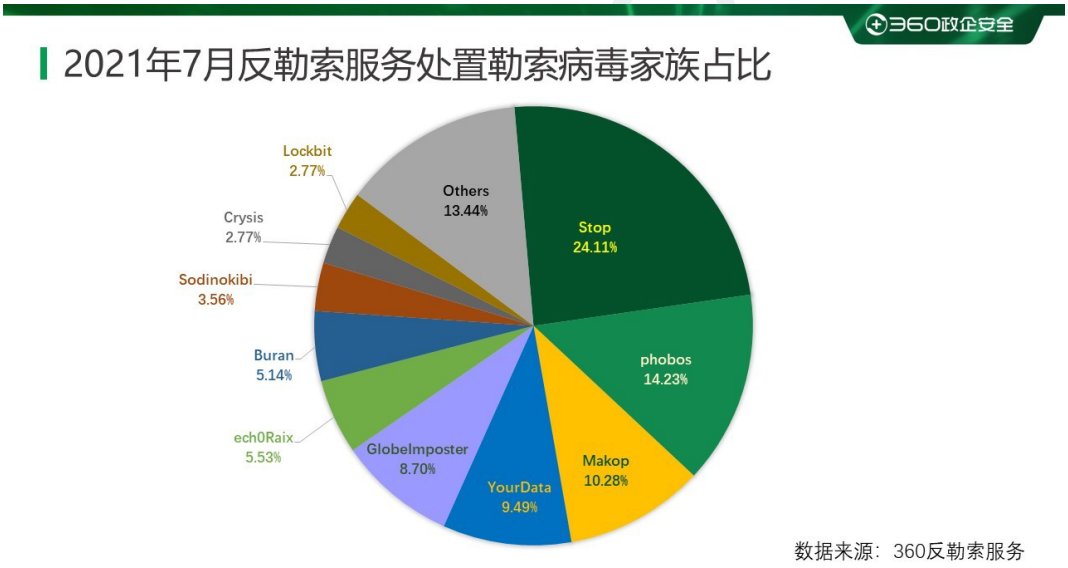
2021 年 7 月，全球新增的活跃勒索病毒家族有:BlackMatter、Grief、AvosLocker、nohope、GoodMorning、MiniWorld、FancyLeaks、LegionLocker、LockBit2.0 等勒索软件。本月还发现 Linux 版本的 HelloKitty 正对安装 VMWare ESXI 的服务器发起攻击。

此外，本月发现 DarkSide 家族重命名为 BlackMatter，而 DoppelPaymer 重命名为 Grief。AvosLocker 可能和 Avaddon 是同一批人运营，而目前双重勒索病毒中最为活跃的一个家族是 LockBit2.0。

2 感染数据分析

针对本月勒索病毒受害者所中勒索病毒家族进行统计，Stop 家族占比 24.11% 居首位，其次是占比 14.23% 的 phobos，Makop 家族以 10.28% 位居第三。

本月 GlobeImposter 家族比较罕见的掉出前三，同时本月通过匿隐僵尸网络进行传播的 YourData 以及针对网络存储设备进行攻击的 ech0Raix 勒索软件有较大的上涨。

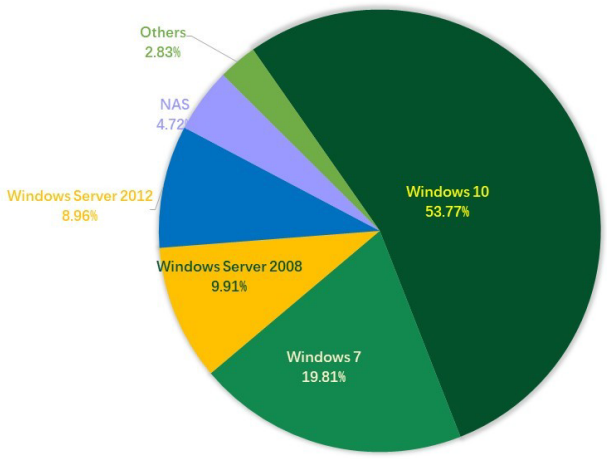


数据来源：360反勒索服务

对本月受害者所使用的操作系统进行统计，位居前三的是：Windows 10、Windows 7 以及 Windows Server 2008。

360政企安全

2021年7月受勒索病毒影响操作系统占比

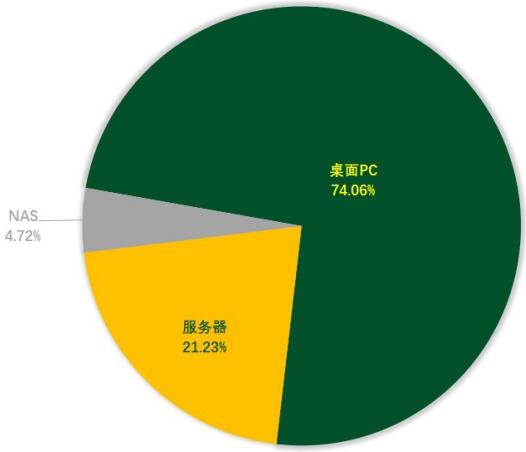


数据来源：360反勒索服务

2021 年 7 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型仍以桌面平台为主，与上月相比无较大波动。本月针对 NAS 设备的攻击事件依然较多，导致其占比有所上涨，建议受害者立即提高设备登录口令的复杂度。若使用的 NAS 设备品牌为威联通，则还应及时对 HBS 多媒体软件进行升级。

360政企安全

2021年7月反勒索服务被感染系统类型占比



数据来源：360反勒索服务

3 勒索病毒疫情分析

3.1 Kaseya 遭 REvil 供应链攻击，100 万个系统被加密，购恢复文件需支付 7000 万美元的赎金

REvil 勒索团伙在暗网数据泄露网站发布了一则声明："周五（2021.07.02）我们对 MSP 提供商发起了攻击，超过 100 万个系统被感染。如果任何人想要协商通用解密器——我们的价格是 7000 万美元的 BTC，那我们将公开发布解密器解密所有受害者的文件，然后每个系统都能在一小时内得到恢复。如果您对此类交易感兴趣——请使用受害者系统中留下的'readme'文档与我们联系。"

除通用解密器的报价，REvil 还对不同类型的受害者报出了不同赎金：针对 MSP(管理服务提供商) REvil 索要 500 万美元，而向其客户则索要 4 万到 4.5 万美元作为赎金。此次攻击事件影响了多个托管服务商及其一千多名客户。其中瑞典最大连锁超市 Coop 因此次事件导致收银系统被感染，被迫关闭了 500 家商店。

针对此次事件调查事，REvil 利用 Kaseya VSA 服务器中的漏洞来访问安装在客户系统中的 VSA 设备，然后通过被感染设备转向所有连接的工作站和公司网络，并安装有效载荷并加密客户文件。该漏洞并非未知漏洞，Kaseya 正在替其用户发布补丁，但不幸的是还是被 REvil 先一步利用了。这次攻击事件不仅是近两年来感染设备量最大的一次，同时也创造了索要赎金金额最大的记录。

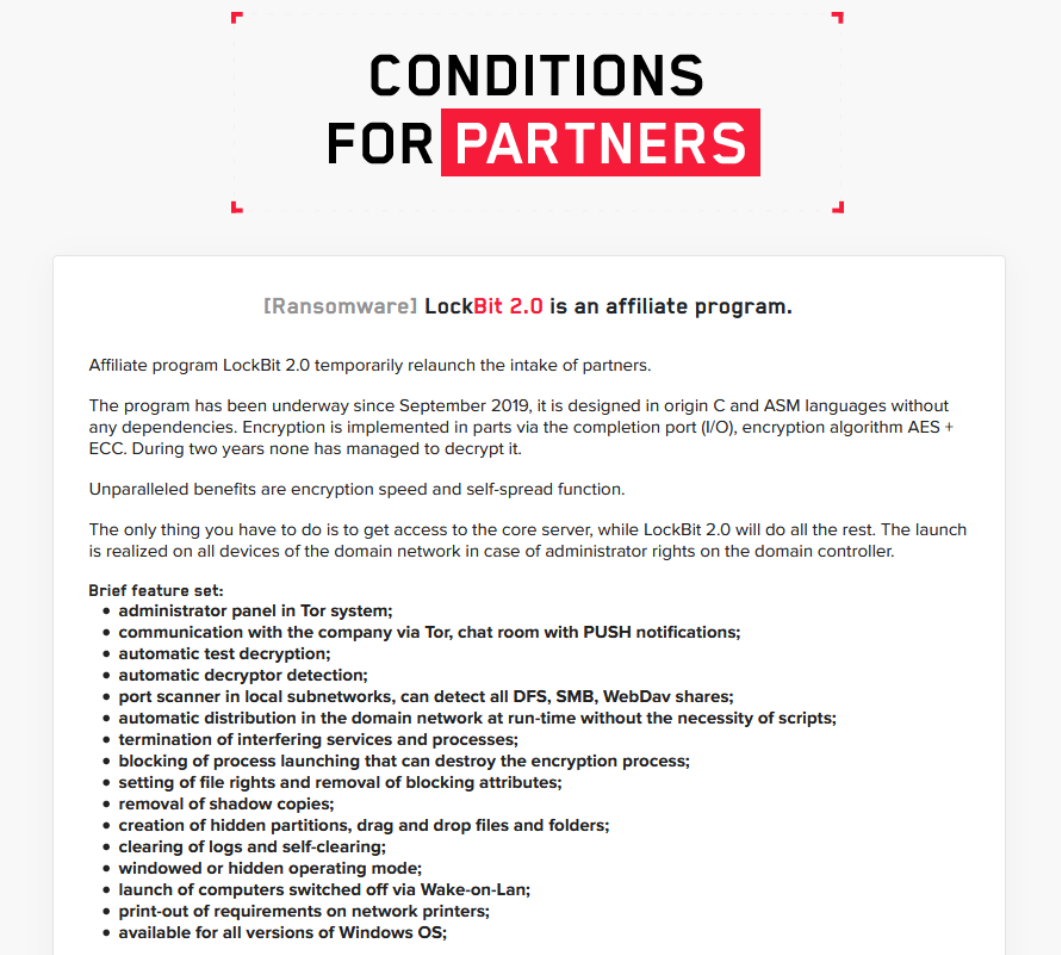
大部分受害者均拒绝向黑客支付赎金——在 7 月中旬仅有两名受害者向黑客妥协，而 7 月底，Kaseya 从受信任的第三方手中获取到了通用解密工具，可以协助此次受攻击影响的设备免费解密文件。

3.2 宣称速度最快的 LockBit 2.0 本月极度活跃

7 月中旬，已消失 6 个月的 LockBit 在其数据泄露网站发布一条新闻宣布更新版本为 2.0。其中最引人注意的是该家族宣称是加密文件最快的勒索软件，并提供了 2.0 版本和其他 34 个勒索软件的加密速度对照表格。同时还会为其攻击者支提供名为"DESITET" 的数据软件，攻击者可通过该软件压缩、上传文件用户文件，作者宣称可在 20 分钟内上传 100GB 数据。在之前发现的版本中，该家族窃取数据利用到了第三方软件 MegaSync。而在今年 6 月份时，RagnarLocker 勒索家族还曾利用 MegaSync 来公开发布受害者数据，不过当时 MegaSync 很快做出反应，删除了该攻击者账户并取消了链接的访问权限。所以猜测也正是由于这个原因，Lockbit 2.0 选择了一个新的数据软件来窃取数据。

Encryption speed comparative table for some ransomware - 18.07.2021 (added Avos & Hive)							
PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD							
Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130	110468
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808	81797
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59	100171
Nephilim	31 Aug, 2020	75 MB/s	22M	1D 12H 40M	No	3061	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930	110026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460	random extension
Avos	18 Jul, 2021	29 MB/s	59M	4D 2H	No	402	79486

同时该勒索软件还在新闻中提到，此次的最新版本具有自传播能力。该勒索软件通过使用 Active Directory 组策略自动加密 Windows 域。



本月该勒索软件家族已成为活跃度最高的勒索病毒家族之一。截止目前为止已有 62 个企业/组织的数据遭到该家族的窃取，该家族最高一天曾连续公布 12 个受害企业/组织名单。目前该数据泄露网上仅保留 40 名受害者信息，由此可推测已有 22 名受害者向该勒索软件团伙支付了赎金。

3.3 匿影僵尸网络协 YourData 勒索软件再度来袭

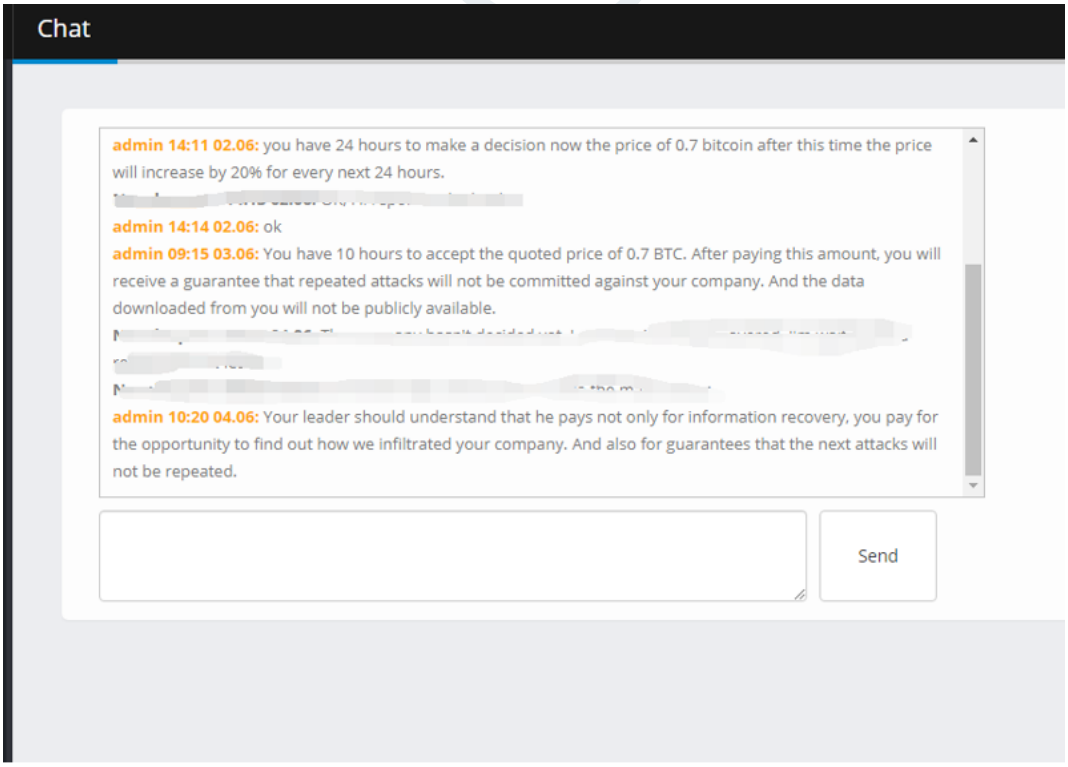
近日 360 安全大脑监控到 YourData 勒索病毒开始采用匿影僵尸网络进行传播 (该僵尸网络还曾传播过 WannaRen 以及 CryptoJoker 勒索病毒家族)，该家族又被称作 Hakbit、Thanos 家族，最早出现于 2019 年 11 月。但在 2021 年 1 月中旬之

前，国内极少出现被该家族或变种攻击案例。2021 年 1 月开始在国内出现该家族的变种，由于早期其后缀虽一直更新，但在国内传播时使用到的邮箱均为 your-data@RecoveryGroup.at，被命名为 YourData。

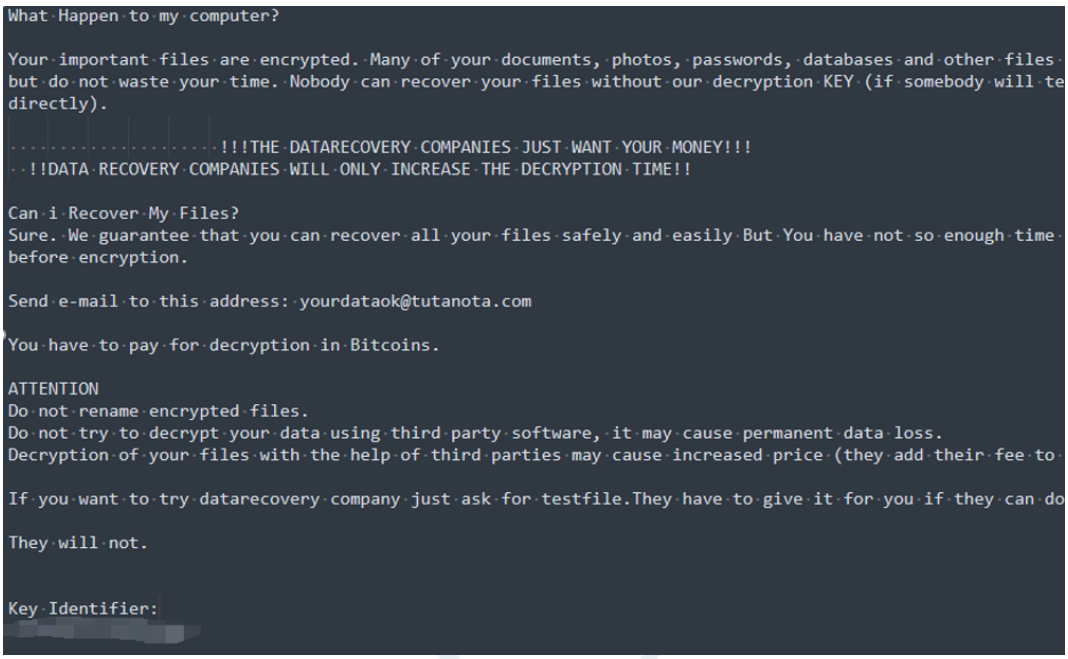
该病毒演变过程如下：

- 2021 年 1 月份开始，该变种开始在国内开始采用暴力破解远程桌面口令进行传播，并不具备任何针对性的投放勒索病毒。
- 2021 年 4 月份开始，发现该家族开始针对性的进行投放勒索软件，使用带有受害者公司名特征的字符串作为后缀，重命名被加密文件。同样采用暴力破解远程桌面口令进行传播。
- 2021 年 7 月份开始，发现该家族开始通过匿隐僵尸网络进行传播，不具体针对性，但是传播量有大幅度提升。

进行针对性攻击时，该家族在生成的勒索提示信息中不仅给出了邮箱联系方式，还给为受害者提供了一个网址，可和黑客进行即时通信。黑客给受害者 24 小时的时间，若不能在 24 小时内支付 0.7BTC 的赎金，解密文件所需费用将提升 20%.



此次利用匿影僵尸网络投放的勒索病毒生成的勒索提示信息，仅提供邮件地址供受害者联系。



3.4 DoppelPaymer 勒索软件重命名为 Grief 卷土重来

在 DarkSide 袭击美国最大的燃料管道运营商之一的 Colonial Pipeline 后，Doppel-Paymer 的活动开始下降。5 月开始其数据泄露网站未曾更新过受害者消息，近日发现 DoppelPaymer 进行品牌重塑后，重命名为 Grief(又叫 Pay)。两者有较多相似之处：

1. 两者共享相同的加密方式。
1. 相同的分发渠道 (Dridex 僵尸网络)。
1. 高度相似的代码，采用相同的加密算法 (RSA2048 和 AES-256)。
1. 均使用欧盟通用数据保护条例 (GDPR) 作为警告，未付款的受害者仍将因违规而面临法律处罚。
1. 数据泄露站点上的防止爬虫的验证码等。

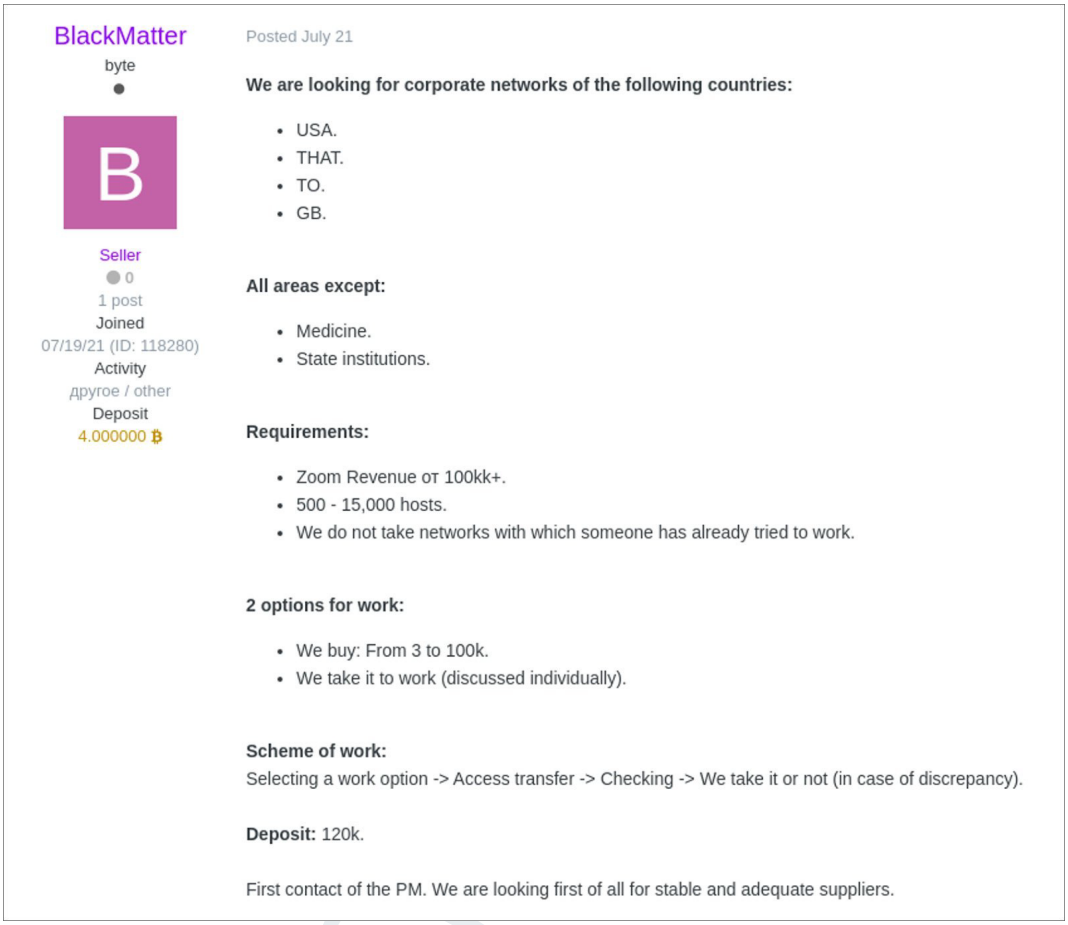
该家族最早的信息是从 2021 年 6 月开始的，但被捕获到的样本的编译时间为 5 月 17

日。同时该家族接受赎金时仅支持 XMR 虚拟货币，采用此虚拟货币很大程度是为了避免被追溯。目前已出现受害者，其中 Clover Park 学区被索要价值 35 万美元的 XMR。

3.5 DarkSide 更名为 BlackMatter 再度活跃，目标瞄准资产超 1 亿美元企业

在 DarkSide 袭击美国最大的燃料管道运营商之一的 Colonial Pipeline 后不久，便关停了所有的基础设施，并销声匿迹。7 月发现一新型勒索软件 BlackMatter(由 DarkSide 重命名而来) 开始在网络犯罪论坛开始发布各种广告招募合作伙伴，并声称同时拥有 REvil 和 DarkSide 的最佳功能。

该团伙在攻击受害者的同时，还积极的从其他攻击者那里购买网络访问权限以发起新的勒索攻击。该家族曾在网络犯罪论坛发布消息称，其主要目标是那些盈利超过 1 亿美元，网络中存在 500-15000 台设备的公司。



BlackMatter
byte

B

Seller
0
1 post
Joined
07/19/21 (ID: 118280)
Activity
другое / other
Deposit
4.000000 ฿

Posted July 21

We are looking for corporate networks of the following countries:

- USA.
- THAT.
- TO.
- GB.

All areas except:

- Medicine.
- State institutions.

Requirements:

- Zoom Revenue от 100kk+.
- 500 - 15,000 hosts.
- We do not take networks with which someone has already tried to work.

2 options for work:

- We buy: From 3 to 100k.
- We take it to work (discussed individually).

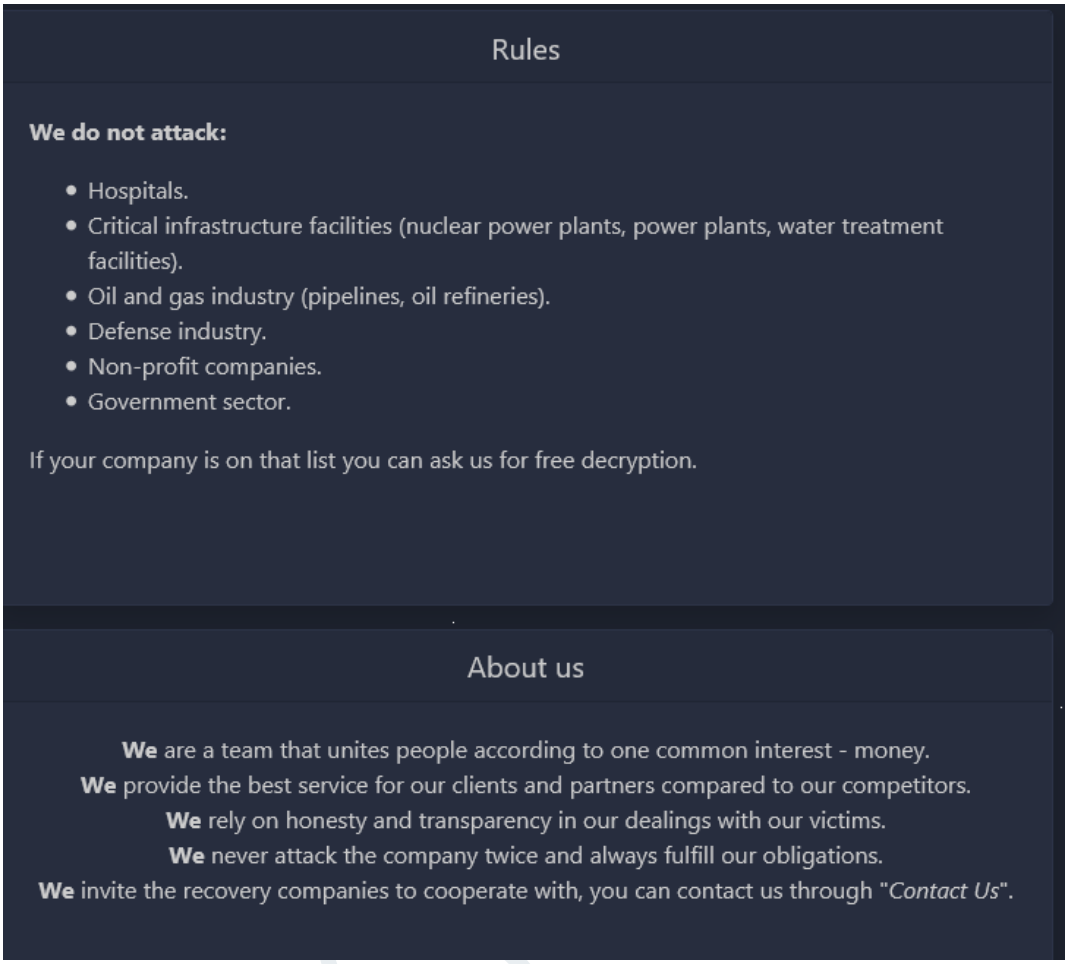
Scheme of work:
Selecting a work option -> Access transfer -> Checking -> We take it or not (in case of discrepancy).

Deposit: 120k.

First contact of the PM. We are looking first of all for stable and adequate suppliers.

该勒索病毒不仅支持在 Windows 上运行，还支持在 Linux 和 EXSi 服务器上运行。目前已出现受害者被攻击，并且已有受害者向 BlackMatter 支付 400 万美元的赎金。从其数据泄露网站发布的消息看，该家族声称不会攻击以下行业，并承诺若以下行业不幸中招，会提供免费的解密工具：

- 医疗行业
- 关键基础设施（核电站、发电厂、水处理设施）
- 石油和天然气工业（管道、炼油厂）
- 非盈利公司
- 政府部门



Rules

We do not attack:

- Hospitals.
- Critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities).
- Oil and gas industry (pipelines, oil refineries).
- Defense industry.
- Non-profit companies.
- Government sector.

If your company is on that list you can ask us for free decryption.

About us

We are a team that unites people according to one common interest - money.
We provide the best service for our clients and partners compared to our competitors.
We rely on honesty and transparency in our dealings with our victims.
We never attack the company twice and always fulfill our obligations.
We invite the recovery companies to cooperate with, you can contact us through "*Contact Us*".

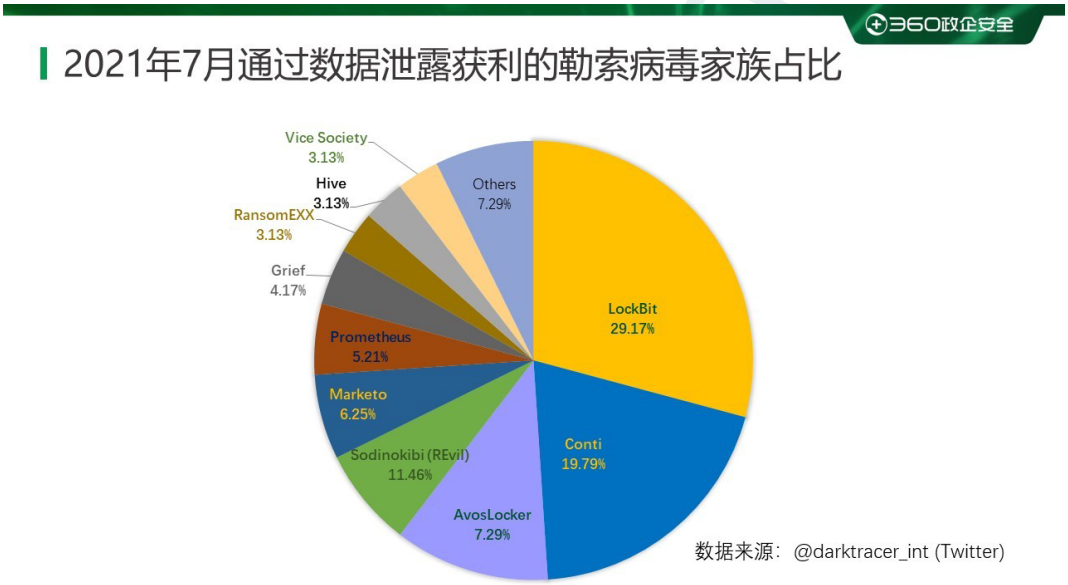
4 黑客信息披露

以下是本月收集到的黑客邮箱信息：

k3n3dy@xmpp.cz	GoodMorning9@cock.li	ustedesfil@safeswiss.com
raincry@dr.com	johnlo@techmail.info	willettamoffat@yahoo.com
keepcry@mail.con	recupes@tutanota.com	GooodMorning@tutanota.com
recofile@mail.ee	tedydecrypt@elude.in	JessMalibu@protonmail.com
Zeus1@msgsafe.io	helpguarantee@aol.com	yourdata@RecoveryGroup.at
3292987166@qq.com	mrreturn@ctemplar.com	cryptodancer@onionmail.org
dragon520@mail.me	slamhelp123@gmail.com	devos_support@pressmail.ch
Handi@firemail.cc	AsupQue@protonmail.com	fushenkingdee@tutanota.com
kingkong2@tuta.io	diniaminius@winrof.com	GooodMorning1@tutanota.com

k3n3dy@xmpp.cz	GoodMorning9@cock.li	ustedesfil@safeswiss.com
Naver@firemail.cc	recofile@mailfence.com	Forexexchane@protonmail.com
norahghnq@gmx.com	chickenfried@keemail.me	Goood.Morning@mailfence.com
chaziz@firemail.cc	decryptionwhy@india.com	protoshak140@protonmail.com
ecoding141@tuta.io	irrelevantly@aliyun.com	Goood.Morning1@mailfence.com
greenoffer@aol.com	justiceinfo@disroot.org	martingarrix@nonpartisan.com
datos@onionmail.org	soterissylla@wyseil.com	nohopeproject@protonmail.com
desmcmorran@aol.com	yourdataok@tutanota.com	troublemaker113@tutanota.com
greenoffer1@aol.com	greenoffer1@tutanota.com	troublemaker113@mailfence.com
nomanscrypt@tuta.io	kabayaboo@protonmail.com	bob_marley1991@libertymail.net
AsupQue@tutanota.com	managerhelper@airmail.cc	slamransomwareasistance@gmail.com

当前，通过双重勒索模式获利的勒索病毒家族越来越多，勒索病毒所带来的数据泄露的风险也越来越大。以下是本月通过数据泄露获利的勒索病毒家族占比，该数据仅为未能第一时间缴纳赎金或拒缴纳赎金部分（因为第一时间联系并支付赎金的企业或个人不会在暗网中公布，因此无这部分数据）。



以下是本月被双重勒索病毒家族攻击的企业或个人。若未发现被数据存在泄露风险的企业或个人也请第一时间自查，做好数据已被泄露准备，采取补救措施。

dimeo	Geneva, Ohio	Arabian Cargo Group
imasa	Stevens & Lee	Breydons Solicitors
cegos	Talbert House	Pesquera Exalmar SAA

dimeo	Geneva, Ohio	Arabian Cargo Group
KASEYA	Paxton Access	ensingerplastics.com
Walsin	Paxton Access	Dragon Capital Group
Alcedo	aris-services	cecengenharia.com.br
Bamford	cometgroup.be	Commune De Villepinte
ALBIOMA	kennen.com.ar	Heller Injury Lawyers
CHADDAD	betonlucko.hr	swiftlogistics.com.my
Beckley	anderscpa.com	Virginia Defense Force
habasit	Techni+Contact	Belperio Clark Lawyers
matchmg	siro-group.com	europeanaccounting.net
Gulf Oil	The Wild Rabbit	creditoycaucion.com.ar

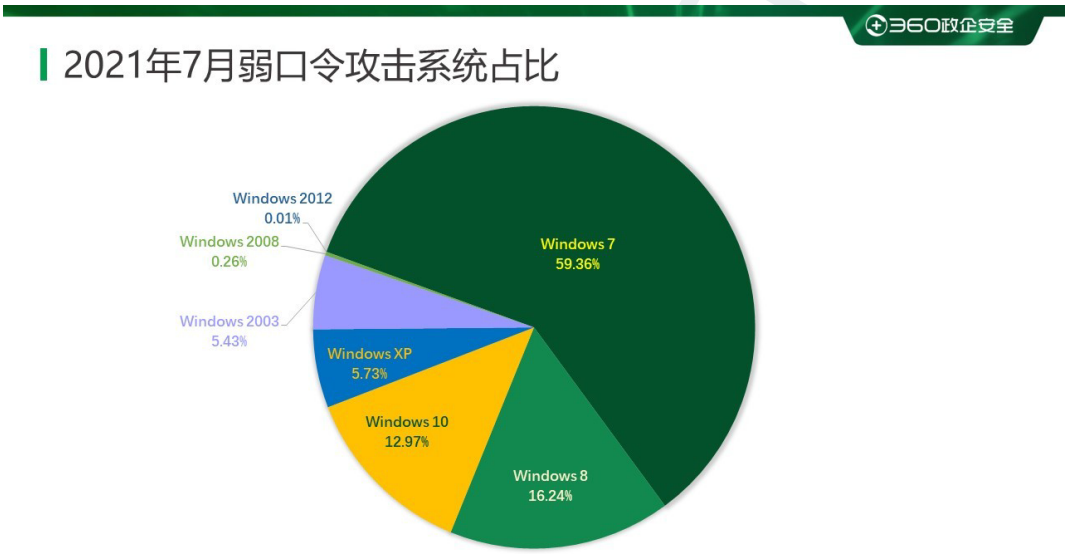
dimeo	Geneva, Ohio	Arabian Cargo Group
Hx5, LLC	Mambrino S.A.C.	sahintoptangida.com.tr
DiaSorin	Gateway College	classicalmusicindy.org
keltbray	INSERM-TRANSFER	Sierra Air Conditioning
friedrich	grupodismar.com	kuk.de / KREBS + KIEFER
PCM Group	f **	Florida Sugar Cane League
BHoldings	vincents.com.au	Walter's Automotive Group
Cinépolis	SAC Wireless Inc	Elm3 Financial Group, LLC
Actiontec	Sandhills Center	Nottingham City Transport
infovista	Home in Brussels	Haftpflichtkasse Darmstadt

dimeo	Geneva, Ohio	Arabian Cargo Group
Jhillburn	Grupo DINA S.A.	GATEWAY Property Management
HUF GROUP	Phoenix Services	Artas Holding / Artas Insaat
Daylesford	riostarfoods.com	South Carolina Legal Services
inocean.no	modernbakery.com	Century 21 Gold Key Realty, Inc
IBC24 News	Agrokasa Holdings	Walter's Mercedes-Benz of Riverside
apg-neuros	Aquazzura Firenze	Trifecta Networks & CloudFirst Labs
ccz.com.au	Revision Skincare	On logistics Services Algeciras, S.L
Mega Vision	spiralfoods.com.au	Corporación Nacional de Telecomunicación

dimeo	Geneva, Ohio	Arabian Cargo Group
supplyforce	cspmould-stampi.it	SALZBURGER EISENBAHN TRANSPORT LOGISTIK GmbH
Colligan Law	WT Microelectronics	Orange County Chrysler Jeep Dodge Ram Dealership

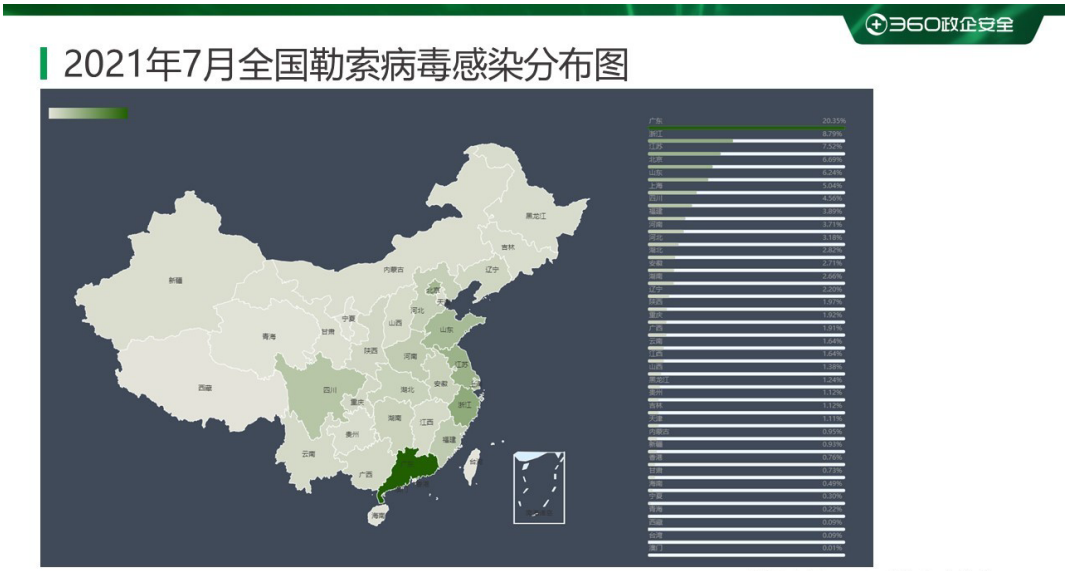
5 系统安全防护数据分析

通过将 2021 年 6 月与 7 月的数据进行对比，本月各个系统占比变化均不大，位居前三的系统仍是 Windows 7、Windows 8 和 Windows 10。



数据来源：360反勒索服务

以下是对 2021 年 7 月被攻击系统所属地域采样制作的分部图，与之前几个月采集到的数据进行对比，地区排名和占比变化均不大。数字经济发达地区仍是攻击的主要对象。



数据来源：360系统安全防护

通过观察 2021 年 7 月弱口令攻击态势发现，RDP 和 MYSQL 弱口令攻击在总体量级层面无较大变化。而利用 MSSQL 进行传播勒索的家族本月的感染量也有大幅度的下降——例如上个月的 GlobeImposter 家族。

数据来源：360系统安全防护

6 勒索病毒关键词

以下是本月上榜活跃勒索病毒关键词统计，数据来自 360 勒索病毒搜索引擎。

- devos：该后缀有三种情况，均因被加密文件后缀会被修改为 devos 而成为关键词。但月活跃的是 phobos 勒索病毒家族，该家族的主要传播方式为：通过暴力破解远程桌面口令成功后手动投毒。

- eking：属于 phobos 勒索病毒家族，由于被加密文件后缀会被修改为 eking 而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。

- Makop：该后缀有两种情况, 均因被加密文件后缀会被修改为 makop 而成为关键词:

- 属于 Makop 勒索病毒家族，该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。

- 属于 Cryptojoker 勒索病毒家，通过"匿隐"进行传播。

- gujd：属于 Stop 勒索病毒家族，由于被加密文件后缀会被修改为 gujd 而成为关键词。该家族主要的传播方式为：伪装成破解软件或者激活工具进行传播。

- zzla: 同 gujd。

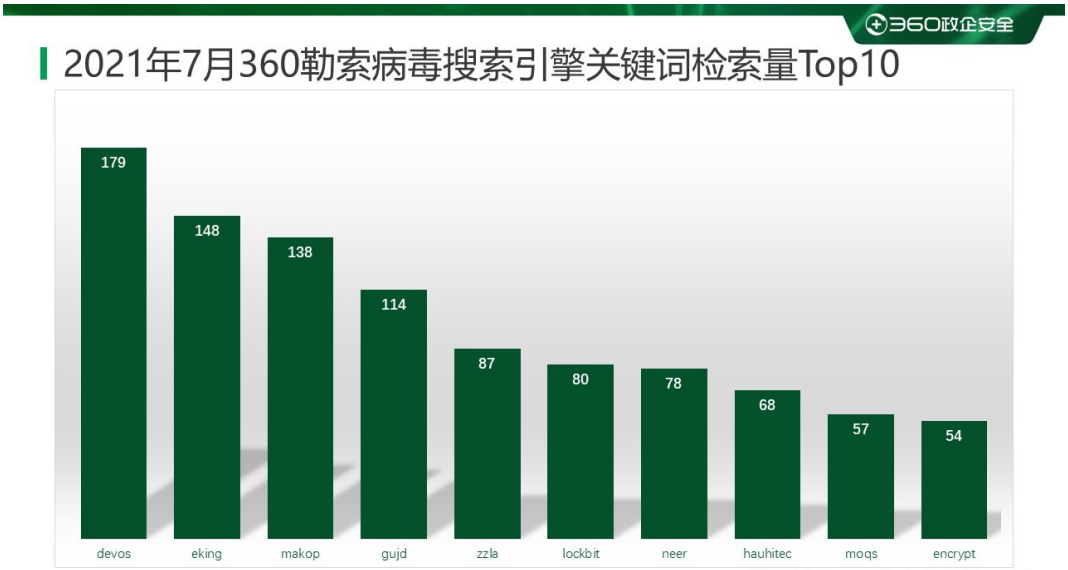
- Lockbit：Lckbit 勒索病毒家族，由于被加密文件后缀会被修改为 lockbit 而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。

- neer：同 gujd。

- hauhitec：属于 CryptoJoker，由于被加密文件后缀会被修改为 hauhitec 而成为关键词。通过"匿隐"僵尸网络进行传播。

- moqs: 同 gujd。

- encrypt：该后缀被很多家族均使用过，但在本月活跃的是 ech0Raix 勒索软件，由于被加密文件后缀会被修改为 encrypt 而成为关键词。该家族针对网络存储设备 NAS 进行攻击，主要通过弱口令攻击以及漏洞攻击进行传播。



数据来源：360勒索病毒搜索引擎

解密大师从解密大师本月解密数据看，解密量最大的是 CryptoJoker，其次是 Gand-Crab。使用解密大师解密文件的用户数量最高的是被 Stop 家族加密的设备，其次是被 Crysis 家族加密的设备。!

7 安全防护建议

面对严峻的勒索病毒威胁态势，360 安全大脑分别为个人用户和企业用户给出有针对性的安全建议。希望能够帮助尽可能多的用户全方位的保护计算机安全，免受勒索病毒感染。

一、 针对个人用户的安全建议

对于普通用户，360 安全大脑给出以下建议，以帮助用户免遭勒索病毒攻击。

(一)养成良好的安全习惯

1) 电脑应当安装具有高级威胁防护能力和主动防御功能的安全软件，不随意退出安全软件或关闭防护功能，对安全软件提示的各类风险行为不要轻易采取放行操作。

2) 可使用安全软件的漏洞修复功能，第一时间为操作系统和浏览器，常用软件打好补丁，以免病毒利用漏洞入侵电脑。

3) 尽量使用安全浏览器，减少遭遇挂马攻击、钓鱼网站的风险。

4) 重要文档、数据应经常做备份，一旦文件损坏或丢失，也可以及时找回。

5) 电脑设置的口令要足够复杂，包括数字、大小写字母、符号且长度至少应该有 8 位，不使用弱口令，以防攻击者破解。

(二)减少危险的上网操作

1) 不要浏览来路不明的色情、赌博等不良信息网站，此类网站经常被用于发起挂马、钓鱼攻击。

2) 不要轻易打开陌生人发来的邮件附件或邮件正文中的网址链接。也不要轻易打开

扩展名为 js 、vbs、wsf、bat、cmd、psl 等脚本文件和 exe、scr、com 等可执行程序，对于陌生人发来的压缩文件包，更应提高警惕，先使用安全软件进行检查后再打开。

3) 电脑连接移动存储设备（如 U 盘、移动硬盘等），应首先使用安全软件检测其安全性。

4) 对于安全性不确定的文件，可以选择在安全软件的沙箱功能中打开运行，从而避免木马对实际系统的破坏。

(三)采取及时的补救措施

1) 安装 360 安全卫士并开启反勒索服务，一旦电脑被勒索软件感染，可以通过 360 反勒索服务寻求帮助，以尽可能的减小自身损失。

二、针对企业用户的安全建议

(一)企业安全规划建议

8 时间线

2021-08-09 360 高级威胁分析中心发布通告

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360AISA 全流量威胁分析系统

针对微软本次安全更新，360AISA 已基于流量侧提供对应检测能力更新，请 AISA 用户联系 techsupport@360.cn 获取更新，尽快升级检测引擎和规则，做好安全防护工作。

A.2 360 安全卫士

Windows 用户可通过 360 安全卫士实现对应补丁安装、漏洞修复、恶意软件查杀，其他平台的用户可以根据修复建议列表中的安全建议进行安全维护。
360CERT 建议广大用户使用 360 安全卫士定期对设备进行安全检测，以做好资产自查以及防护工作。

A.3 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

A.4 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全

产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。