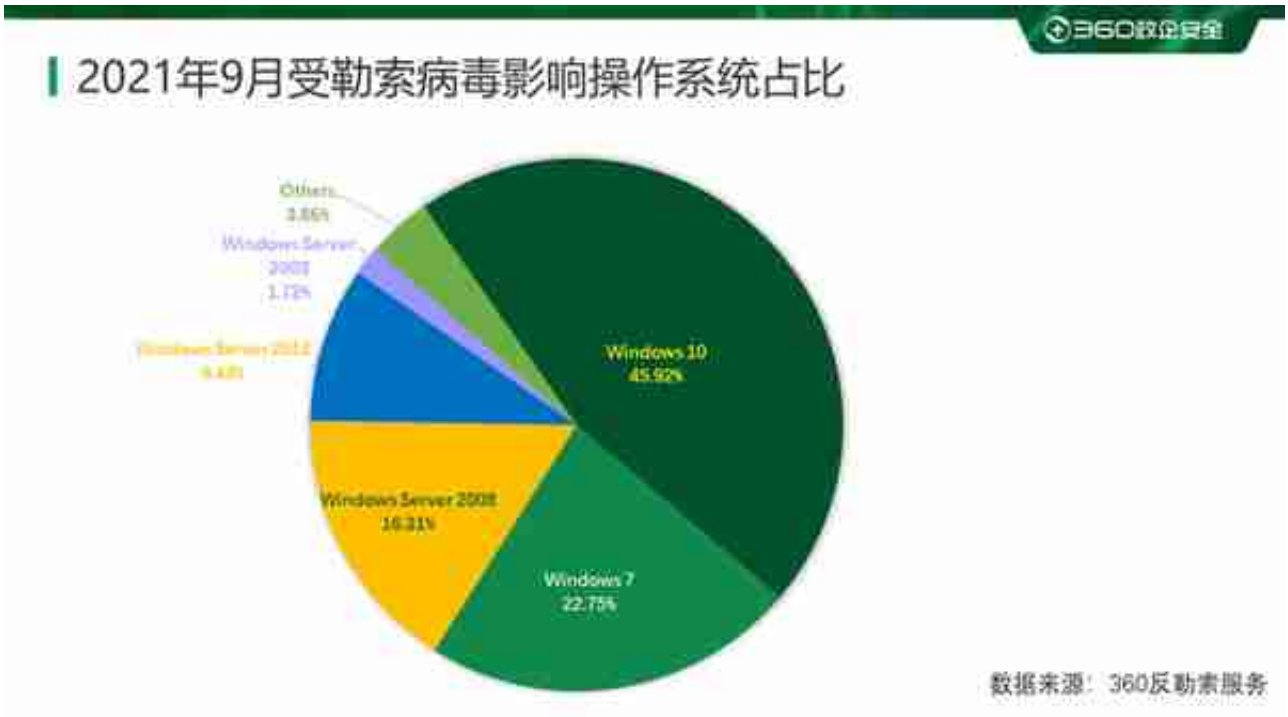
勒索病毒传播至今，360反勒索服务已累计接收到上万勒索病毒感染求助。随着双重勒索的快速增长，企业数据泄露风险不断上升，数百万甚至上亿赎金的勒索案件不断出现。勒索病毒给企业和个人带来的影响范围越来越广，危害性也越来越大。360安全大脑针对勒索病毒进行了全方位的监控与防御，为需要帮助的用户提供360反勒索服务。

2021年9月，全球新增的活跃勒索病毒家族有:AtomSilo、BlackByte、Groove、Sodinokibi(REvil)、Colossus等勒索软件。其中AtomSilo的数据泄露网站与Black Matter的数据泄露网站高度相似，两者可能存在密切关系；Groove勒索软件由Babuk部分核心成员参与运营，并创建了一个名为RAMP的暗网论坛；消失近两月的Sodinokibi(REvil)在本月正式回归；Colossus勒索软件的勒索提示信息结构与Sodinokibi(REvil)相似，采用双重勒索模式运营。

感染数据分

针对本月勒索病毒受害者所中勒索病毒家族进行统计，phobos家族占比18.95%居首位，其次是占比17.32%的BeijingCrypt，Stop家族以14.05%位居第三。

本月BeijingCrypt勒索感染量有大幅度的上升，从8月份的4.06%上升至本月的17.32%。另外，在本月底该家族出现新的变种，将被加密文件后缀修改为“.520”。



本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

系统为主，与上月相比无较大波动。

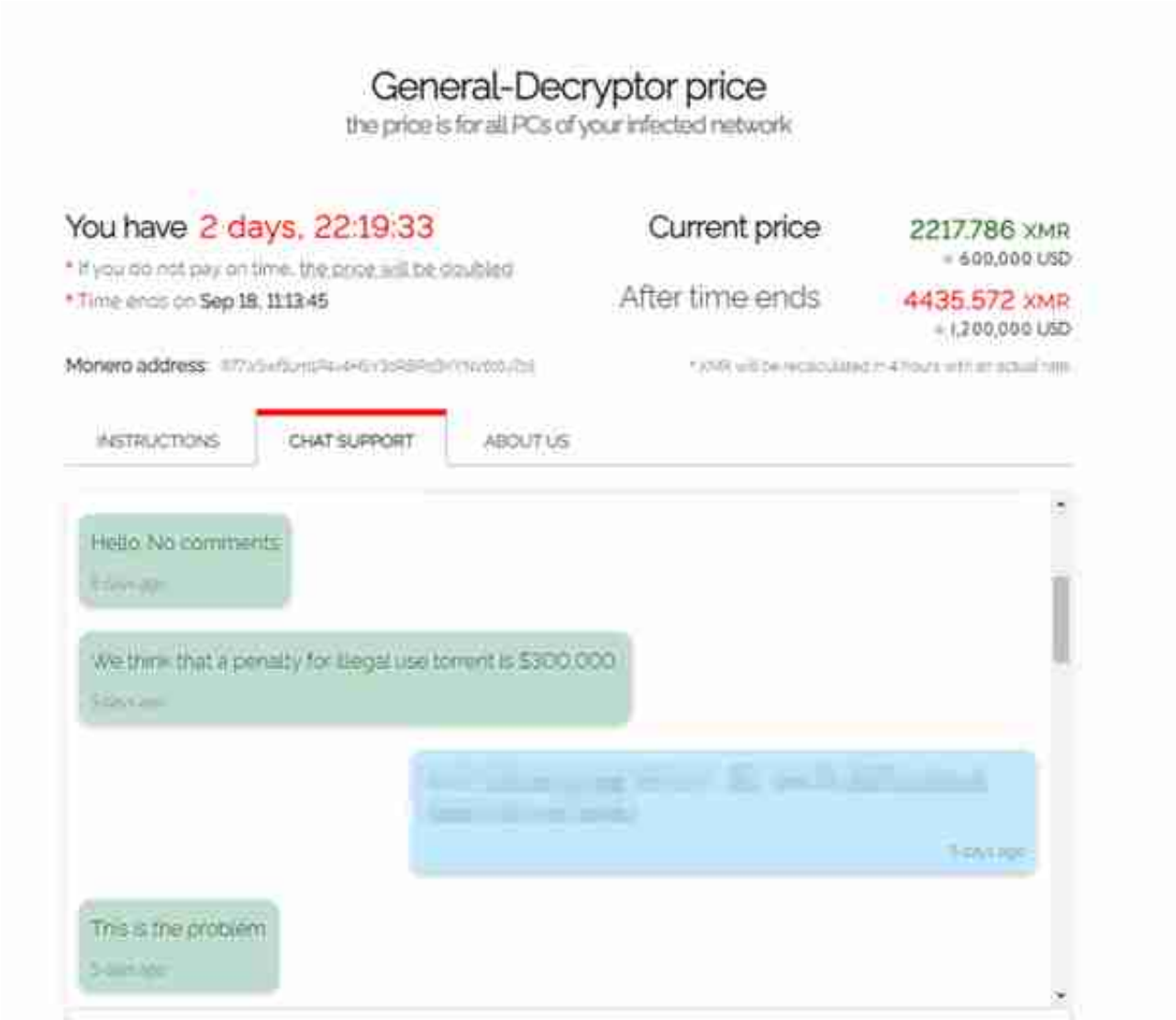


图1. 受害者与Sodinokibi(REvil)赎金谈判页面

就在Sodinokibi(REvil)勒索软件宣布回归后不久，国外执法部门通过特殊渠道获取到了该家族早期的密钥，并决定在该家族发起第二波攻击之前为受害者提供解密方案（解密工具仅能解密7月13日之前被加密的文件）。目前360解密大师已加入了对Sodinokibi(REvil)的解密支持，受害者可以使用解密大师解密文件。

图3. 受害者与BeijingCrypt作者赎金谈判邮件

根据此次受害者所从事的行业进行分析，被攻击的受害者中大部为零售行业。通常利用远程桌面进行传播的勒索病毒并不具备针对某特定行业的定向投放能力，这是首次出现通过远程桌面转播勒索病毒具有如此强的行业针对性。

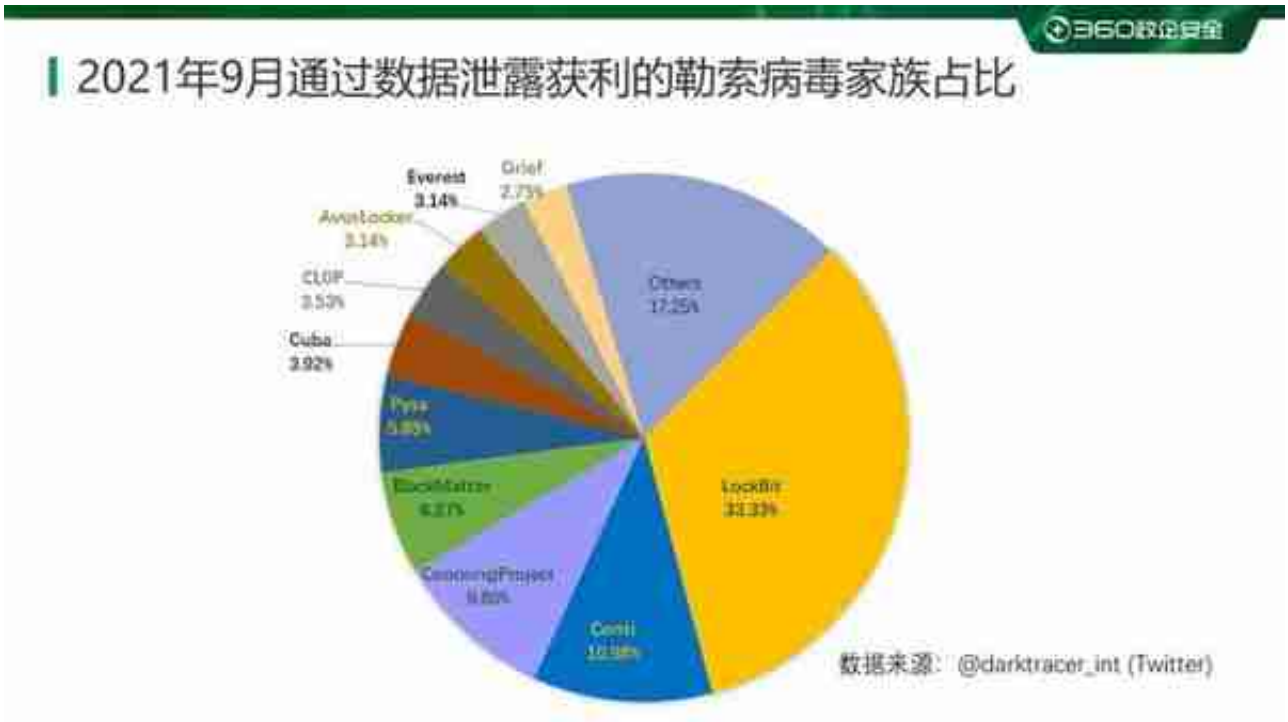
勒索软件团伙内部分裂，Groove勒索软件诞生

Babuk勒索团队在2021年4月攻击华盛顿警方后产生内部分歧。其管理员决定公布从警方手中获取到的敏感信息用于宣传，但部分成员拒绝这一行为，认为泄露警方数据会带来大量不好的影响。而在管理员泄露数据后，该组织出现分裂——部分成员创建RAMP论坛，而另一些人员启动了BabukV2勒索攻击。在6月Babuk勒索生成器被泄露，9月Babuk成员将Babuk源代码在暗网公开发布。

本月，一名ID为“Orange”的黑客在RAMP发布了一篇文章，文章中包含12856台设备上近50万个用户的Fortiner VPN凭证。根据IP定位其所属国家，发现有11.89%的设备来自中国。同时还观察到Groove勒索软件的数据泄露网站发布了一篇指向RAMP论坛关于Fortinet VPN凭证泄露的文章，猜测其团伙公开这些凭证的目的是想吸引更多的黑客参与该勒索软件活动。

图5. Ragnar_Locker拒绝与数据恢复公司谈判公告

在Ragnar_Locker发布此消息后，Grief勒索团伙也发布公告将拒绝来自第三方的谈判、拒绝二手交易，如果遇到来自数据恢复公司的谈判，他们将直接销毁数据。



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。

AZA	hbfinanse.pl	CROMOLOGY SERVICES
HBE	atstrack.com	WEST TREE SERVICE
HABI	ebarc.adv.br	Bellissima Fashions
AMAX	grupowec.com	MangaDex - MangaDex
VIVEA	ibes-gmbh.de	odeffinancierasa.hn
Dohuk	noone.com.au	Irish Pioneer works
Andel	drsdoors.com	shop.jerryleigh.com
UUOOI	novotech.com	hotelservicepro.com
Axley	C & C FRANCE	scisairsecurity.com
Bulley	Aria Systems	transrendufense.com
Saurer	IJmond Werkt	pulmuonewildwood.com
Nwdusa	dataspeed.it	ATIVY CYBER SECURITY
Butali	RTI Surgical	royalporcelain.co.th
lrz.de	GEO-Alpinbau	Jesse Engineering Co
Phminc	newhotel.com	One Community Health
Ohagin	Famous Supply	mitchellsternlaw.com
Linkmfg	benner.com.br	Unified Technologies
iibg.ca	SUNSETHCS.COM	Office Star Products
calsoft	ROC Mondriaan	Unione Reno Galliera

Fountain	jaylon.com.au	rabbalshedekraft.com
Wibernet	alderking.com	Chamco Industries Ltd
nrpa.org	crystalvalley	Trust Capital Funding
AUTO.RIA	cheadlelaw.com	soenen-golfkarton.com
myyp.com	GENESISNET.COM	Haverhill High School
parcoinc	cansmart.co.za	EQUITY TRANSPORTATION
Meriplex	Steel Projects	Pramer Baustoffe GmbH
SI Group	BRPRINTERS.COM	United Health Centers
Meditopia	BCP Securities	Macdonald Devin, P.C.
ASSU 2000	Actief-Jobmade	papierswhitebirch.com
comebi.mx	Citrocasa GmbH	buffingtonlawfirm.com
pi-hf.com	hoffsuemmer.de	peabodyproperties.com
Grupo SAN	daylewis.co.uk	FEINBERGLAWOFFICES.COM
Southland	Memory Express	Global Crypto Exchange
Elementia	hoistcrane.com	novohamburgo.rs.gov.br
ds.net.au	Schultheis-ins	EMPIRICAL-RESEARCH.COM
Real Time	Potter Concrete	johncockerillindia.com
PeakLogix	remedios.lawyer	Huali Industrial Group
KESSEL AG	hpe-konstanz.de	Cedar Grove Composting
PRECREDIT	Dassault Falcon	River City Construction
Grupo GSS	STORAFILE.CO.UK	BLUEBONNETNUTRITION.COM
amista.cz	ohiograting.com	Modern Testing Services
advint.com	Xmedicalpicture	Plastipak Holdings, Inc.
advint.com	miller-rose.com	Hörmanseder Stahlbau GmbH
Journality	TPI Corporation	coldwellbankerhubbell.com
Ellerboeck	SCREEN Holdings	Marans Weisz & Newman, LLC
Miningbase	CasagrandeGroup	Bumper to Bumper Autoparts
Technicote	j-addington.com	Barlow Respiratory

BPATPA.COM	northstarak.com	Hospital Spartanburg & Pelham OB-GYN
tesa46.com	Amphenol Canada	Charles Crown Financial Ltd
ofplaw.com	robsonstreet.ca	The Plastic Forming Company
gahesa.com	IN2 Engineering	DEBTIN CONSULTANTS (PTY) LTD
cimico.net	advantecmfs.com	PrÃ©-Sal PetrÃ³leo S.A. PPSA
aathonrton	Vera Wang Group	Whitefish River First Nation
esopro.com	Karavan Trailers	Annonces et Vous Particuliers
dykman.com	LJ Hooker Aspley	VIVA Formwork and Scaffolding
51talk.com	Align Technology	Eisvogel Hubert Bernegger GmbH
sete.co.uk	Iraqi Government	Afohs Club â□ “ Enjoy The Pride
anasia.com	autohausdaehn.de	Beat The System With Beatchain
denark.com	callabsolute.com	northwoods & spectrumfurniture
DataXsport	Woodlake Unified	South Carolina State University
fugybat.fr	callabsolute.com	Запатченные fortinet точки входа
Bob Poynter	NASCO Industries	Spiezle Architectural Group Inc.
ludofact.de	LA-Martiniquaise	Gaulhofer Industrie-Holding GmbH
barolit.com	geda-produkte.de	C-PatEx - Cryptocurrency Exchange
prototal.se	texasacehvac.com	Primary Residential Mortgage inc.
cimaser.com	nitropiso.com.mx	Greensville County

		Public Schools
rlsblaw.com	Pacific City Bank	Cristália - Indústria Farmacêutica
BÖWE SYSTEC	denverhousing.org	Société de transport de l'Outaouais
drhrlaw.com	Creditriskmonitor	Marquez Brothers International, Inc.
iiservz.com	russellwbho.co.uk	United Carton Industries Company Ltd
glenroy.com	wijnendeclerck.be	Hamilton Duncan Armstrong | Law firm
abcp.org.br	BONTEMPI VIBO SPA	Ward Arcuri Foley & Dwyer | Law Firm
riscossa.it	Clay County Clerk	Lancaster Independent School District
tes-amm.com	Jakes Finer Foods	EAP Films and Theatres Private Limited
Aluflexpack	franklinempire.com	Fimmick CRM Hong Kong (www.fimmick.com)
BOSCA S.p.A	TaxLeaf Corporate	Instituto Nacional de Medicina GenÃ³mica
Minjar Gold	YASH Technologies	Catalogue des cours de TÃ©lÃ©com SudParis
vlastuin.nl	calautomotive.com	the NET - Northeast Tennessee Media Group
wortmann.de	Gershman Mortgage	South African National Space Agency: SANSA
ch13bham.com	Bar-Ilan University	The Virginia Federation of Republican Women
WPSD Local 6	Betson Enterprises	Municipal Government of Calamba, Philippines
Sarmad Steel	robinwoodortho.com	Canadian Warmblood Horse Breeders Association - Home
Berding-weil	Pulmuone Co., Ltd.	Synthetic Roofing Products and Information - InterWrap
suenco.co.th	Pines Ford Lincoln	Politeknik Elektronika

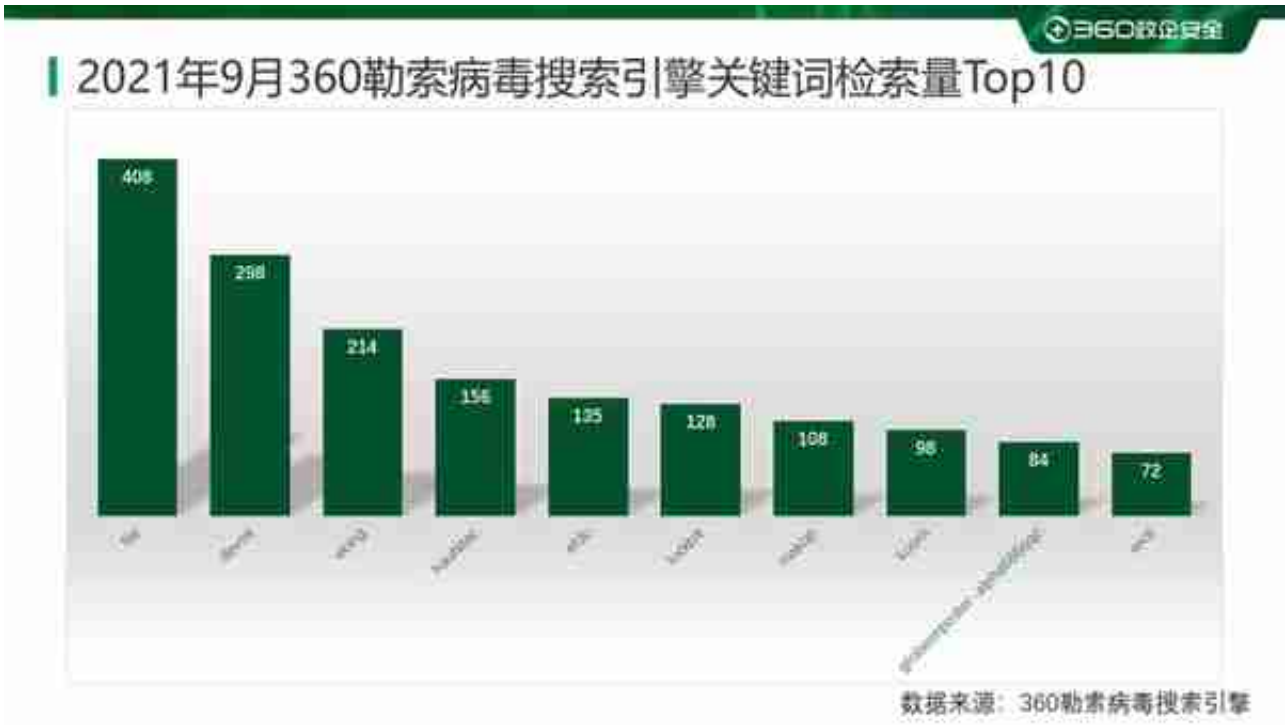
tovogomma.it	PowerGrid Services	Negeri Surabaya | Emerging Technology Freewallet | Multi-currency Online Crypto Wallet for BTC, ETH

表格2. 受害组织/企业

系统安全防护数据分析

通过将2021年8月与9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。

通过观察2021年9月弱口令攻击态势发现，RDP和MYSQL弱口令攻击整体无较大波动。MSQQL属于正常的波动范围。



解密大师

从解密大师本月解密数据看，解密量最大的是Sodinokibi（REvil），其次是CryptoJoker。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。