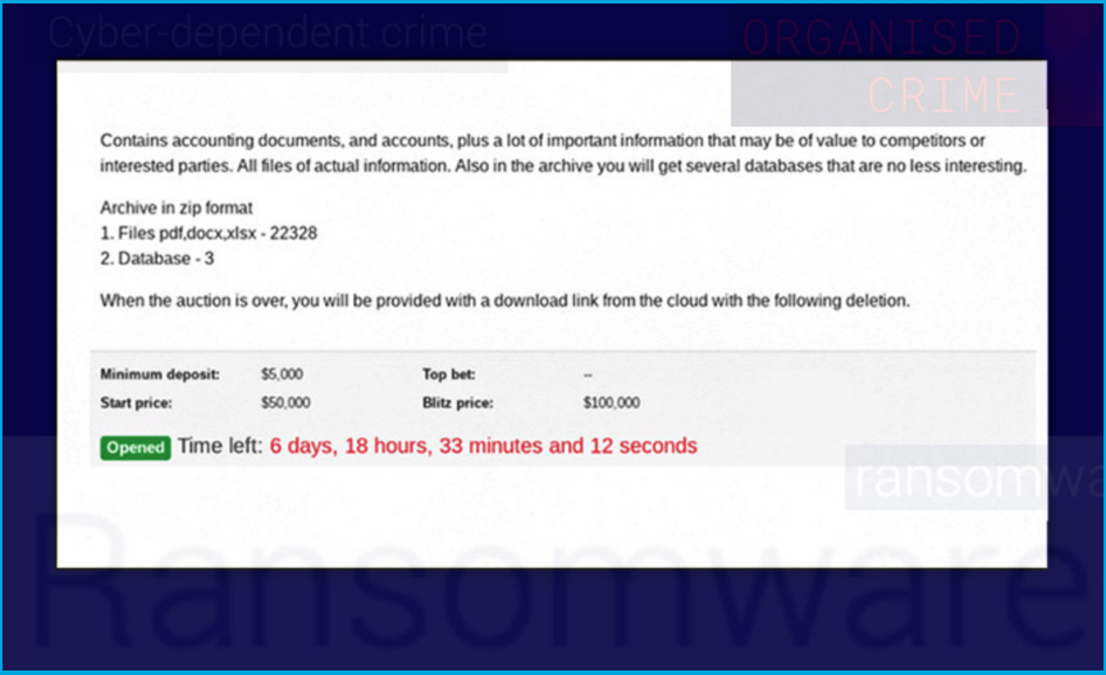
kindred

Security Newsletter

12 October 2020

Subscribe to this newsletter

Ransomware: Cybercrime Public Enemy No. 1



Contains accounting documents, and accounts, plus a lot of important information that may be of value to competitors or interested parties. All files of actual information. Also in the archive you will get several databases that are no less interesting.

Archive in zip format
1. Files pdf,docx,xlsx - 22328
2. Database - 3

When the auction is over, you will be provided with a download link from the cloud with the following deletion.

Minimum deposit:	$5,000	**Top bet:**	–
Start price:	$50,000	**Blitz price:**	$100,000

Opened Time left: 6 days, 18 hours, 33 minutes and 12 seconds

Ransomware continues to solidify its position as the No. 1 online threat targeting public and private organizations. Seeking maximum returns, more gangs have moved beyond opportunistic attacks to target organizations with what experts call "post-intrusion ransomware." Meanwhile, many victims fail to report such crimes to police, hampering their ability to disrupt these attacks.

This week, incident response firm Kroll said that, so far this year, of the many security incidents it has investigated for clients, ransomware has been the leading cause, accounting for 35% of incidents. Last year, for example, an attack against Eurofins Scientific, one of the largest forensic labs in the U.K., created a backlog of 20,000 forensic samples - including DNA and blood samples - that needed analyzing as part of ongoing criminal cases. Even after the lab paid a ransom to its Ryuk-wielding attackers, getting its systems restored and the backlog cleared led to months of delays.

You don't need an MBA to divine the driver for attackers: Ransomware continues to generate massive revenue, thanks to many organizations opting to pay a ransom in return for a decryption tool or a promise from attackers to destroy stolen data or to not leak it. Thus, an illicit business model continues to be validated and to draw new adherents. The highest-impact threat we're seeing is what we'd call post-intrusion ransomware. Post-intrusion ransomware is distinct from more opportunistic crypto-locking malware attacks, in which individual users might open an attachment that would encrypt everything on their PC, delete the originals and then flash a ransom note. Instead, they're following what we would class as APT-style tactics that we used to attribute to nation-states, to do things to get into environments, get complete control of the environment and then take it over.

Another innovation has been to steal data before crypto-locking systems and then threaten to leak the stolen data unless victims pay. Ransomware incident response firm Coveware has reported that, from April to June, based on the thousands of incidents it investigated for clients, 22% of ransomware cases involved data exfiltration.

More than a dozen ransomware operators now have name-and-shame sites or use leaking or auction sites to try and pressure victims into paying. These include Maze - which kicked off the trend - as well as Sodinokibi, Ryuk and Egregor. As ransomware attacks continue to surge, then, here's the message from law enforcement agencies to ransomware victims: Please come forward.

Read More on BankInfoSecurity

The State of Ransomware 2020 - Sophos

More #News

- Microsoft: Iranian hackers actively exploiting Windows Zerologon flaw
- Four npm packages found uploading user details on a GitHub page
- Chowbus delivery service breached, hacker emails data to users
- Boom! Mobile falls prey to Magecart card-skimming attack
- Researchers Find Vulnerabilities in Microsoft Azure Cloud Service
- Waterbear malware used in attack wave against government agencies
- Tesla accuses employee of Californian factory sabotage
- Ransomware Attack Hits Clinical Trial Software Vendor
- Wi-Fi security: FBI warns of risks of using wireless hotel networks
- Ransomware threat surge, Ryuk attacks about 20 orgs per week
- Sam's Club customer accounts hacked in credential stuffing attacks
- Amid an Embarrassment of Riches, Ransom Gangs Increasingly Outsource Their Work
- Sophisticated new Android malware marks the latest evolution of mobile ransomware

#Patch Time!

- Android's October 2020 Security Update Patches 48 Vulnerabilities
- Chrome 86 released with password-related security improvements

#Tech and #Tools

- We Hacked Apple for 3 Months: Here’s What We Found
- Best practices for defending Azure Virtual Machines
- Ryuk ransomware: went from an email to domain wide ransomware in 29 hours, asked for over $6 million USD
- OAuth 2.0 Security Best Current Practice
- Enter the Vault: Authentication Issues in HashiCorp Vault
- How to Find Vulnerabilities in Code: Bad Words
- Keeping the sauce secret – Introducing GitLab Watchman and GitHub Watchman
- Raccine - A Simple Ransomware Protection
- Find your unscanned and overexposed shares on-premises with an on-premises scanner

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us