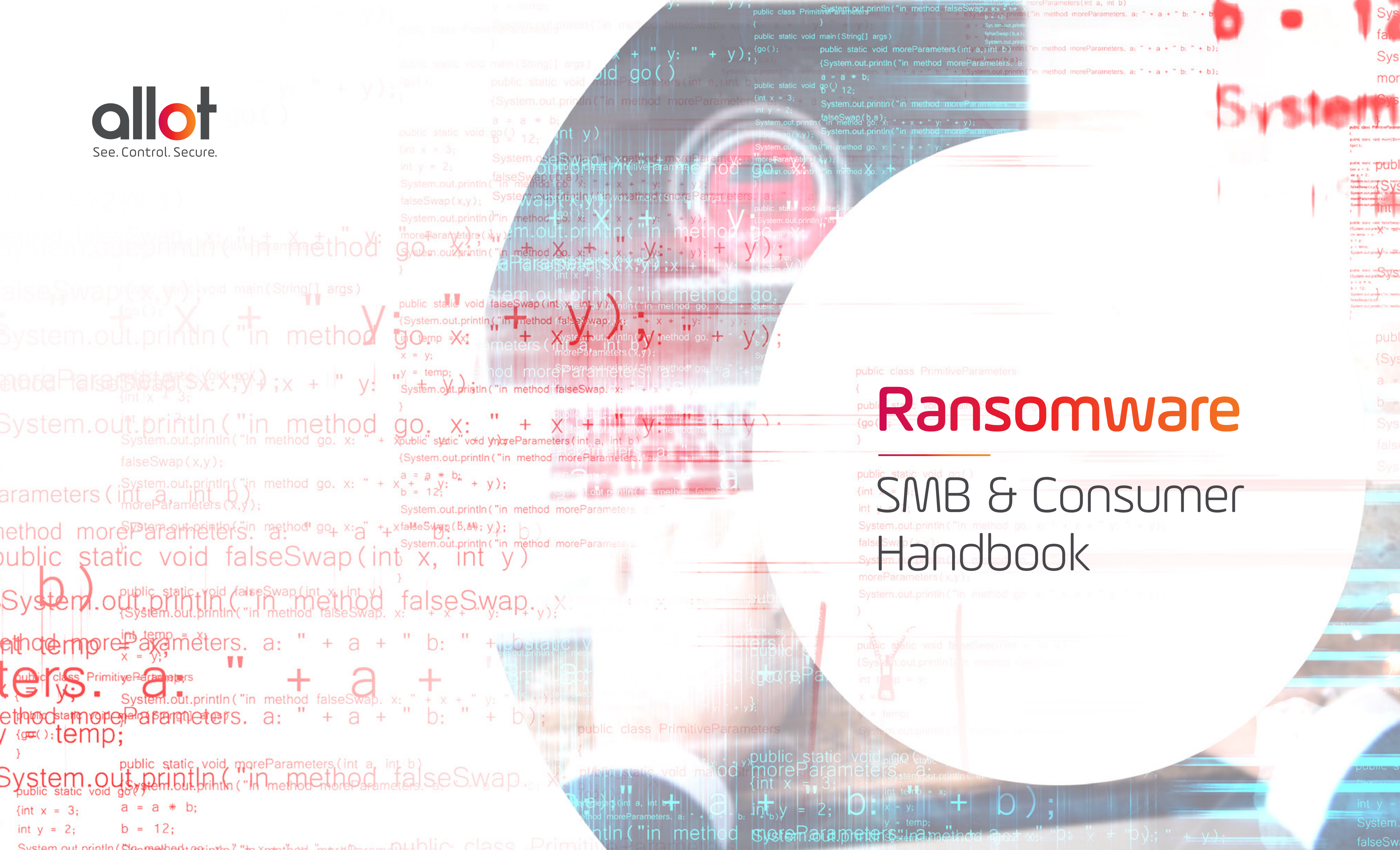
See. Control. Secure.



Ransomware

SMB & Consumer Handbook

public class PrimitiveParameters
ublic static void main(String[] args)
b = 12;

Intro

Ransomware attacks continue to surge. In 2022, ransomware victimized about 70% of businesses, marking a surge from the past five years and the highest reported so far.[1] Cybercrime costs in the United States reached an estimated 320 billion U.S. dollars by 2023, showcasing a remarkable increase of over 300 billion U.S. dollars from 2017 to 2023. This upward trend is projected to persist, with anticipated cybercrime costs reaching around 1.82 trillion U.S. dollars by 2028.[2]

[1] Businesses-ransomware-attack-rate by Statista

[2] Estimated annual cost of cybercrime in the U

What is Ransomware?

Ransomware is a type of malware designed to take over a user's data, systems or entire devices and make them inaccessible until the victim pays a ransom to regain control.

Cybercriminals typically trick unsuspecting victims into installing ransomware by clicking an attachment or link in a phishing email that looks legitimate, or when a victim visits a hacked website.

The rising popularity of Ransomware-as-a-service (RaaS) allows evenless-skilled criminals to employ this tactic on a massive scale - with high reward for little effort and less technical knowledge.

Ransomware attacks on organizations are generally more disruptive than traditional cyberattacks focused on stealing information. They can prevent access to critical data causing a shutdown of part, if not all, of a business operation until the data is restored or replaced.

Types of Ransomware

There are several general categories of ransomware that have varying threat levels and removal methods. We discuss the different types and corresponding removal techniques, but the best defense is operator-delivered, network-native cybersecurity, as provided by Allot Secure, that prevents infection in the first place.

Fake Ransomware

These fake antivirus or PC Cleanup tools pretend to be ransomware and try to scare you into paying for fake removal programs. Scareware is highly uncommon these days, but some of these viruses still exist and many of them are now targeting mobile phones.

If you think you are seeing scareware on your computer or phone, there's a simple way to investigate. See whether you can access your files or folders, such as the items on the desktop or in the My Documents folder. If you can navigate the system and open most files, then you're probably seeing something fake that's just trying to scam you.

How to remove: Scareware is the easiest to get rid of - in most cases, you can remove scareware using standard anti-virus removal tools.

Locking Ransomware

This version of ransomware locks the device and may even display fake messages from law enforcement agencies like the FBI or police or tax authorities, informing the victim that they've detected illegal activity on the computer for which a fine must be immediately paid. While the screen locker won't encrypt or delete your files, you may find yourself forced to perform a system restore.

How to remove: Screen-lockers can be easily removed at little to no cost. At first restart your computer in Safe Mode by following the relevant instructions below:

- **Windows tablet/laptop:** Power button + S at startup
- **Windows desktop PC:** Click restart + hold down Shift on login screen
- **Mac:** Restart + hold down Shift

From there, you should be able to clean up the ransomware using a free malware removal tool like the ones mentioned above.

If that doesn't work, you can perform a system restore to a point before the scareware or screen locker began popping up messages. After you've done this, we recommend running your antivirus software one more time to make sure your system is clean.

To learn more about how ransomware attacks work, read our real-time report on BadRabbit, one of the most popular strains of ransomware.

Encrypting Ransomware

This is the most damaging and therefore alarming type of ransomware. It encrypts user's files with a strong algorithm and presents a ransom note informing victims how to pay (typically in bitcoin or other digital currency) in order to restore access to their assets.

Encrypting ransomware is one of the most significant cyberthreats facing businesses and individuals today. By 2021, global ransomware damage costs are predicted to reach $20 billion. These attacks are becoming increasingly sophisticated, more challenging to prevent, and more damaging to their victims. For example, advanced ransomware will also attempt to encrypt on-line backup copies of local files to increase the likelihood of getting paid.

How to remove: Since this type is much more complicated to deal with, on the next page we'll provide an in-depth guide.

Security Tips to Avoid Ransomware

There are simple security practices you can follow to limit damage by preventing ransomware infections before they strike.

1. The first line of defense is to subscribe to a security service provided by your ISP or mobile operator, ideally Allot Secure.
2. Do not open suspicious email attachments and click on links, even if you think you know and trust the sender - most ransomware is distributed via phishing messages. So if you are suspicious, go directly to the website using your browser instead of clicking on the suspicious link..
3. Make regular offline backups. Since some variants of ransomware can delete backup copies on your computer and network drives, save your files on an external drive or in the cloud. This ensures you don’t lose files if you are targeted by a ransomware attack.
4. Keep your OS and all your software updated and patched.
5. Beware of pirated content and software, which are usually distributed via P2P and torrent sites and can include malware.
6. Use strong and unique passwords for every site.
7. Enable the ‘Show file extensions’ option in the Windows settings on your computer. This will make it much easier to spot potentially malicious files. Stay away from file extensions like ‘.exe’, ‘.vbs’ and ‘.scr’. Hackers can use several extensions to disguise a malicious file as a video, photo, or document (like hot-chics.avi.exe or doc.scr).
8. If you notice any suspicious activity on your computer, disconnect it immediately from the internet or other network connections (such as home Wi-Fi) to prevent the infection from spreading and contact a qualified professional to resolve the issue.

Conclusion

Ransomware is not a new cyberthreat, but it has evolved to become a ubiquitous and serious one, targeting anyone and everyone to bring big profits to its authors. By adopting healthy internet practices, you can minimize your chances of falling victim and spare yourself all the hassle.
If you DO see a ransom note on your screen one day, we hope this guide will help you handle it.

If you are a communications service provider interested in offering security services to your customers, learn more about how Allot can help.

Tell me more »

Disclaimer: We have made every reasonable effort to present accurate information in this guide; however, we are not responsible for any of the results you experience while using it. We cannot assure you that all of the information provided will always be accurate or up to date, nor can we take responsibility for your use of this information.

About Allot

Allot Ltd. (NASDAQ, TASE: ALLT) is a provider of leading innovative network intelligence and security solutions for service providers worldwide, enhancing value to their customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, network-based security services, and more. Allot's multi-service platforms are deployed by over 500 mobile, fixed and cloud service providers and over 1000 enterprises. Our industry leading network-based security as a service solution is already used by over 20 million subscribers around the world. For more information,
visit www.allot.com

allot
See. Control. Secure.

Sep. 2023