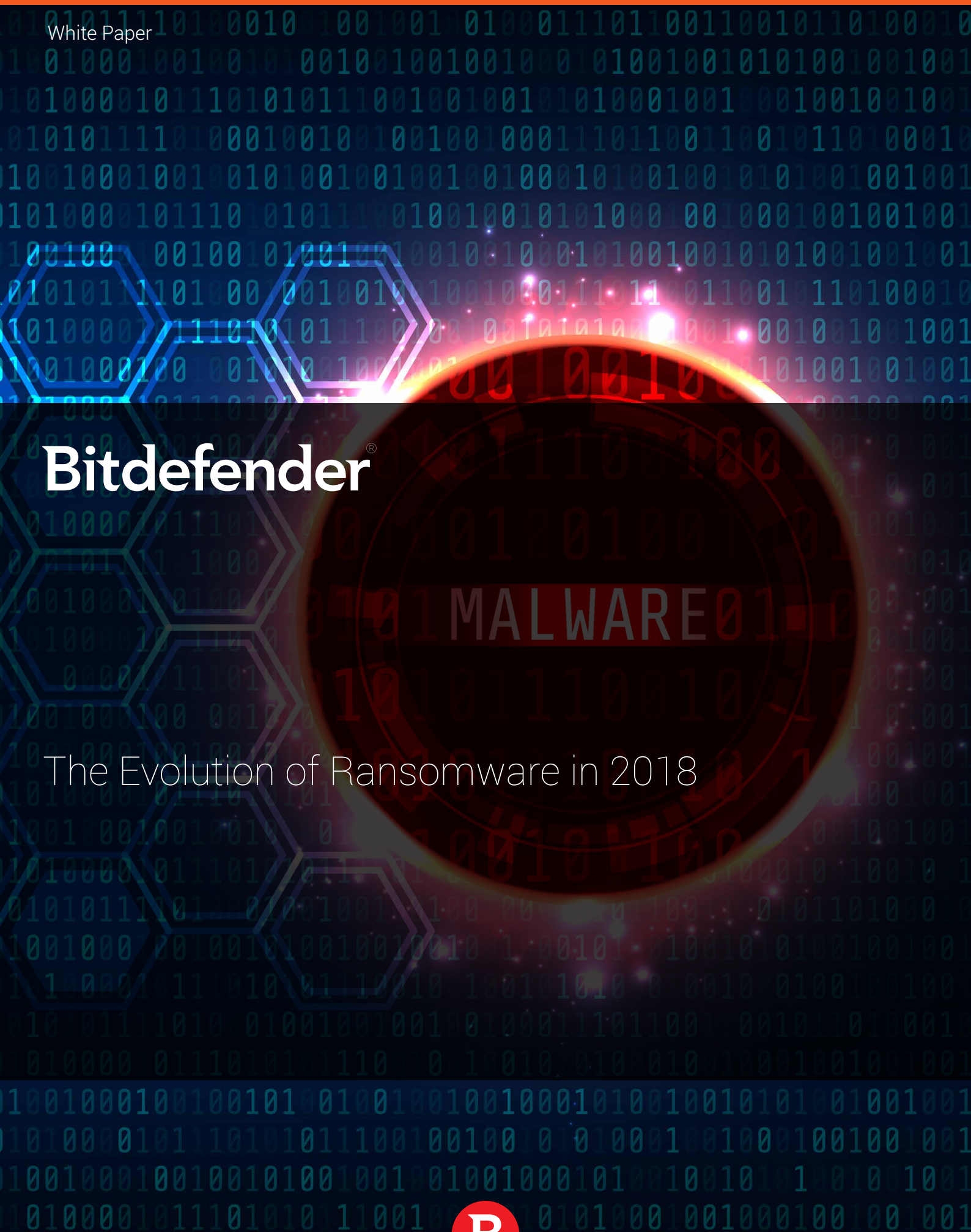
White Paper



Bitdefender®

The Evolution of Ransomware in 2018

Author: Filip Truta, Security Analyst

Executive Summary

In just the past few years, ransomware has evolved from a novelty to the most feared malware of the digital era. Amateur hackers have amassed fortunes thanks to this prolific crypto-viral extortion scheme, but things are beginning to change. Advanced criminals with increasingly sophisticated attack avenues and obfuscation techniques are putting the original small crooks to shame. Today's bad guys not only manage to evade corporate defenses, they are also insatiable in their ransom demands.

Ransomware drains billions from the global economy each year and shows no signs of slowing down. However, the highest cost of a ransomware attack is no longer the ransom itself. Today, the bulk of the financial damage consists of downtime, tarnished reputations and regulatory fines. Depending on operational structure and business model, some organizations cannot recover from a ransomware attack without significant losses. For some businesses, ransomware can spell bankruptcy. For others, it means years of effort to recover. The progressively dangerous nature of ransomware highlights the importance of deploying a multi-layered defensive framework to protect critical data and the IT infrastructure.

This whitepaper analyzes the evolution of attackers' methodology and the industries and geographical areas targeted most by ransomware in 2018. We also look at the year-over-year succession in ransomware families employed by hackers, the most prolific ransomware families in 2018, and take a quick glance at the latest solution to combat ransomware in business environments.

Highlights

Obfuscation through sophistication – ransomware operators are becoming better at their craft

Healthcare in the crosshairs – SamSam made a headline almost every week in H1 2018 as it infected healthcare institutions

GandCrab – the most prevalent ransomware threat in operation, with a 50% share

Bitdefender GandCrab decryptors – recovered data for more than 21,000 victims, saving an estimated $30 million in ransom money

Ransomware stats over a two-year period – 2017 to 2019

Defending your digital infrastructure – how to combat the evolving ransomware threat with a multi-layered defensive framework

Obfuscation through sophistication

In a notable trend in the ransomware world last year, the number of overall infections dropped compared to the year before, but targeted attacks increased as operators switched to more lucrative techniques and campaigns.

Cyber criminals now commonly employ fileless ransomware and multi-stage/component variants. The encryption process grew increasingly randomized and spread out over a longer time, threatening to destroy not just troves of precious data, but the backups as well. To increase the damage to their victims, operators sought to encrypt the very code that a hard drive uses to boot up the computer: the Master Boot Record (MBR).

Polymorphism and fileless delivery avenues create a problem for detection mechanisms. Polymorphic ransomware changes its code between infections, throwing off signature-based security tools. And multi-threaded attacks – provoking a chain reaction that drops the payload before IT can detect the treat – accelerated the encryption process, making it difficult to stop before it was already too late.

Amateur attackers are being driven out of business by sophisticated techniques. Ransomware operators in 2018 learned that, by improving their attack avenues, attack techniques and actual ransomware code, they stand to make far more money while at the same time eliminate 'high-schoolers' from the game. "Spray and pray" techniques have been replaced by "big game hunting" where one big target – usually a hospital or large corporation – gets most of the attention in exchange for a six-figure payout.

Wiper ransomware

Another emergent trend in 2018 was the repurposing of ransomware by attackers. Realizing that businesses would rush to restore operations and only later investigate the attack, bad actors began to use ransomware to conceal themselves in a broader attack. Since ransomware is perfect for scrambling data, why not use it to cover your tracks?

A telltale sign of wiper ransomware is the absence of a ransom note or an unreasonably tedious payment process. These types of attacks need not leverage a completely new binary. Rather, attackers can just take a known ransomware family off the shelf and modify it slightly to serve their goals.

> "It's not uncommon for threat actors to deploy ransomware after they've successfully exfiltrated data. It's actually becoming a relatively common practice for threat actors to cover their tracks by dropping ransomware inside an infrastructure after they've successfully achieved their goals … It will probably become the standard MO for covering tracks."
>
> ***Liviu Arsene, Global Cybersecurity Analyst, Bitdefender***

Healthcare in the crosshairs

Ransomware operators had a particular taste for healthcare institutions in 2018. For the better part of H1 2018, a ransomware family named SamSam made a headline almost every other week for infecting a clinic, hospital, or Electronic Medical Record (EMR) vendor. Governmental institutions were also in SamSam operators' crosshairs. The attackers leveraged a wormable component to gain a foothold onto the targeted infrastructure. Throughout its lifecycle, it is believed SamSam earned more than $6 million for its authors. SamSam was responsible for 32.27% of ransomware infections of healthcare institutions in H1 2018..

SamSam spreads through the web, as well as through Java-coded software, targeting external-facing Remote Desktop Protocol (RDP) servers. It relies on unsophisticated techniques, such as brute forcing credentials, to guess weak passwords and make its way into the network. A wormable component lets it spread laterally to infect other vulnerable systems on the network. The SamSam ransom note displays an ironic "I'm sorry" before asking the victim to pay up.

Key SamSam attacks in 2018

Ransomware attack drives Indianapolis hospital back to pen and paper
New ransomware attack forces hospitals to turn away patients
SamSam ransomware infects Colorado Department of Transportation
Hackers breach Singapore's largest healthcare provider; steal records of 1.5 million patients, including the Prime Minister's
At $17 million, Atlanta network recovery six times more expensive than estimated

It's hard to calculate the exact financial damage an entity incurs after a ransomware attack. The city of Atlanta alone was forced to spend upwards of $17 million after its own SamSam incident. The toll is high, by any margin, across all industries affected by this ransomware family alone. The damage from a ransomware attack is notoriously long-lasting, affecting operations, generating fines, and denting the organization's reputation.

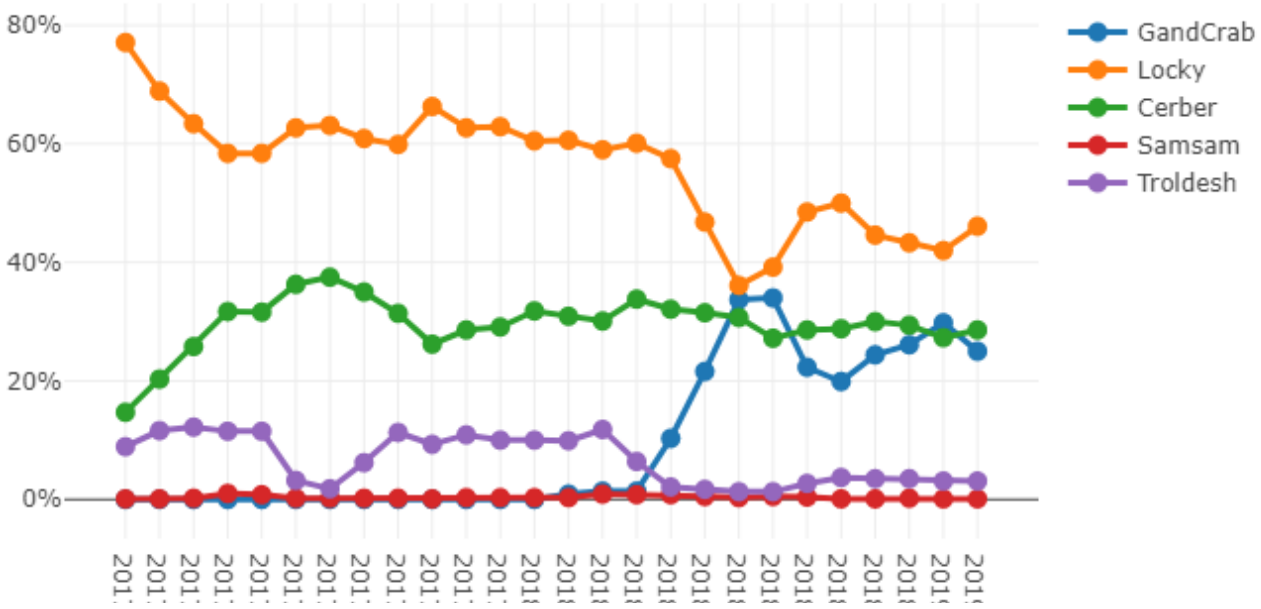
Damage to an organization's image can (and often does) directly impact churn rate. According to a study by Ponemon Institute, healthcare has the highest "abnormal" churn rate of all industries, at 6.7%, followed by finance (6.1%), pharmaceuticals (5.5%), services (5.2%), technology (4.6%), industrial (3.1%), energy (3.0%), communication (2.9%), and education (2.7%). Finally, healthcare institutions are notoriously lagging in cybersecurity practices.

GandCrab – the 'Alpha' ransomware

Ransomware families count in the hundreds while strains number in the thousands. However, only a few names crop up every year in the media, as operators tend to focus on improving flagship ransomware families with a proven track record. For example, 2014 was the year of CryptoLocker, TorrentLocker and CryptoWall. In 2015 and 2016, Fusob took centerstage. 2017 was notorious for the massively viral WannaCry and Petya campaigns. For 2018, bad actors had in store the usual suspects: Locky, Cerber, SamSam, and other infamous names, as well as newcomers such as GandCrab.

> "Significant security incidents are a near universal experience in US healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets … That e-mail continues to be the most frequently reported initial point of compromise is not surprising as phishing e-mails are inexpensive to generate and can be quite accurate in targeting recipients."
>
> 2019 HIMSS Cybersecurity Survey

Without discriminating between targets, GandCrab took the limelight in 2018. The crustacean-themed ransomware stood out of the crowd through almost the entire year of 2018, with victims claimed as early as January. Despite not infecting the most endpoints out there, GandCrab really showed its claws in the second half of 2018, demanding exorbitant ransom sums, up to $700,000 in some cases. While other families dominate the scene in terms of span and number of infections, none made more profit for its authors than GandCrab.



GandCrab evolution relative to other high-profile ransomware names. Jan-Dec 2018

The second half of 2018 saw a surge in GandCrab detections, with October recording the most GandCrab reports.

GandCrab campaigns are operated as-a-service -- the attacker is an "affiliate" in the program and has complete control over the spreading mechanisms that lead to infection. Many GandCrab affiliates attack organizations via exposed Remote Desktop Protocol instances, or by directly logging in with stolen domain credentials. After authenticating on a compromised endpoint, attackers manually run the ransomware and instruct it to spread laterally across the network. With the network infected and the organization's precious data encrypted, the attackers proceed to erase their traces and contact the victim with a ransom demand. There have been reports that GandCrab operators have demanded up to $700,000 per server.

Key GandCrab strengths

- **Powerful affiliate model allows hackers to franchise the ransomware code**
- **Wide choice of attack avenues, from e-mail to exploit kits to manual infection of big game targets**
- **Control over the ransom demand based on how important the infected system to the IT ecosystem**
- **Agile development quickly irons out bugs**
- **Constantly updated to expand on existing functionality**

Compared to other ransomware families, GandCrab has more than one ace up its sleeve. When performing reconnaissance on the victim's system, GandCrab operators can determine the value of the data they are about to hold for ransom. Affiliates then adjust the ransom note for each victim based on the sensitivity of data and tailor a ransom demand to the victim's wallet. If the infected server holds a large database full of sensitive information, the ransom demand can be in the hundreds of thousands, whereas a server with less valuable information might merit a ransom demand as small as $500.

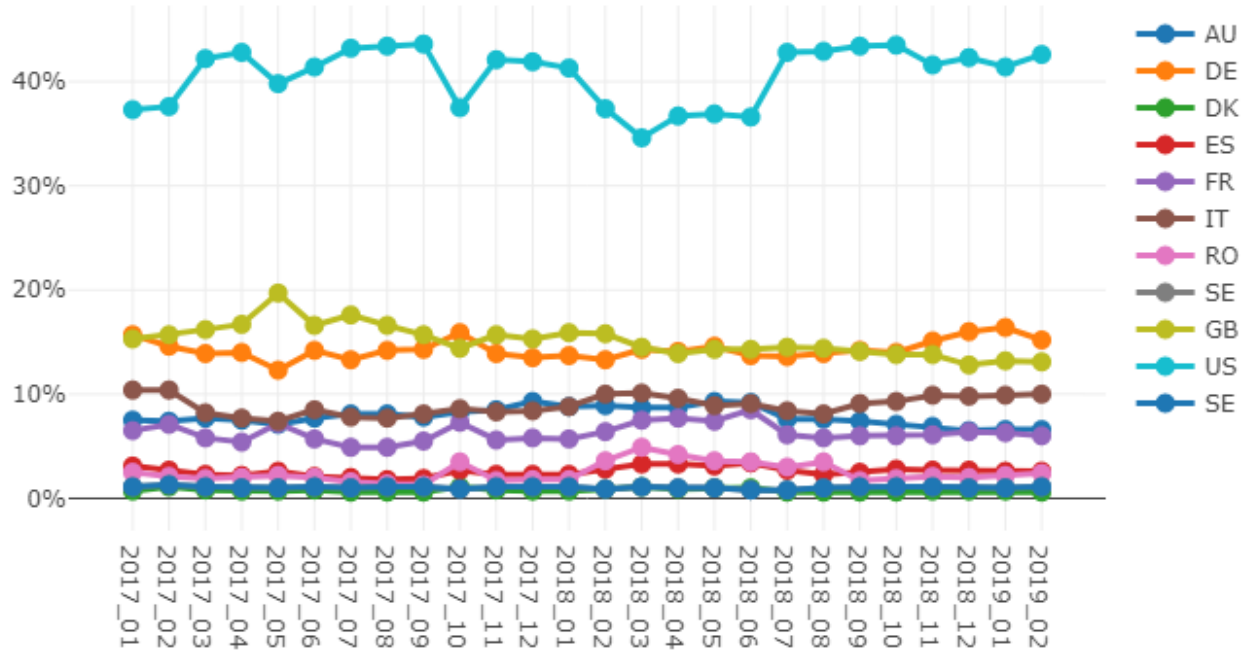
As of late 2018, GandCrab operators updated their spreading mechanisms and affiliation programs, and improved the malware's resilience against cyber-security solutions.

GandCrab decryptors save an estimated $30 million in ransom money

In collaboration with Europol and the FBI, Bitdefender in 2018 developed timely, free-to-download decryptors for most GandCrab variants, recovering precious data belonging to more than 21,000 victims and saving an estimated $30 million in ransom money to date. In the proverbial cat-and-mouse game, operators patched GandCrab in the wake of every new decryptor release.

Countries most affected by ransomware in 2018

Of the countries with the most Bitdefender customers, the United States clearly stands apart, with a 40% share in 2018. In other words, of all the ransomware attacks reported globally in 2018, almost half were reported in the U.S alone. Britain and Germany take the second and third spots, followed by Italy, Australia, France, Romania, Spain, and others.



Defending your digital infrastructure

Hundreds of thousands of malware variants are created daily, with the vast majority used only once before they are modified. Traditional signature-based AV simply cannot keep up. By the time a signature is created, the malware has already changed. These attacks highlight the importance of deploying a multi-layered defensive framework to protect crucial data and the IT infrastructure. Businesses require adaptive layered security solutions that provide multiple anti-ransomware capabilities, having all its layers work together for prevention, detection and remediation of ransomware attacks.

Ransomware writers often use exploit kits that take advantage of un-patched known vulnerabilities to gain a foothold in systems. Security solutions built on machine learning models can make behavioral analysis and prevent ransomware from gaining a foothold in the IT infrastructure, while at the same time provide insights into advanced attacks. Learn more at https://www.bitdefender.com/.

"What ransomware cannot hide is network traffic, which is why during a forensic investigation it's important to cover that aspect as well, as it usually reveals anomalous endpoint behavior, lateral movement, and even communication with C&Cs. Looking for signs that a ransomware infection could be used to cover a data breach should also involve performing a network-level investigation and analyzing all network and endpoint event information dating back to days, weeks and even months prior to the ransomware incident."

Liviu Arsene, Global Cybersecurity Analyst, Bitdefender

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/.

Bitdefender is a global cybersecurity leader protecting over 500 million systems in more than 150 countries. Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for the smart connected home, mobile users, modern businesses and their networks, devices, data centers and Cloud infrastructure. Today, Bitdefender is also the provider of choice, embedded in over 38% of the world's security solutions. Recognized by industry, respected by vendors and evangelized by customers, Bitdefender is the cybersecurity company you can trust and rely on.

Bitdefender-Whitepaper-EvoRan-CREAT3441-en_EN