



From fish tanks to medical files:

Get the facts on cyberattacks

It takes hackers minutes to break into a network, but an average of 279 days for businesses to identify and contain a breach. Don't let a lack of security close you down.



BTS TECHNOLOGIES

IT Services | Phones | Security

“

Someone was fooled by the email from the CEO and used his corporate credit card to send the iTunes gift cards. We lost about \$5,000.”

— Adam A., video game rentals, 150 employees



BTS TECHNOLOGIES

IT Services | Phones | Security

“



**They got someone's
password, and sent an
email to our CFO, who
sent the \$40,000 wire
transfer.”**

**— Bob K., property
management, 150 employees**



BTS TECHNOLOGIES

IT Services | Phones | Security



01

Cyberattacks

Cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.



BTS TECHNOLOGIES

IT Services | Phones | Security

Malware

Malicious software includes spyware, ransomware, worms and viruses.

Spyware

This attack aims to gather information about a person or organization without their knowledge and send such information to hack another entity without the consumer's consent.

Ransomware

This type of malware from cryptovirology threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Viruses

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus. Computer viruses currently cause billions of dollars' worth of economic damage each year, due to causing system failure, wasting computer resources, corrupting data, increasing maintenance costs, or stealing personal information.

Worms

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers.



BTS TECHNOLOGIES

IT Services | Phones | Security

Denial-of-service (DOS) attack

Floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests.

Phishing

The practice of sending fraudulent communications that appear to come from a reputable source, usually through email.

Man-in-the-middle (MITM) attacks

Also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

Zero-day exploit

Hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time.

Structured Query Language (SQL) Injection

Occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out an SQL injection simply by submitting malicious code into a vulnerable website search box.



BTS TECHNOLOGIES

IT Services | Phones | Security



02

Most bizarre hacks:



BTS TECHNOLOGIES

IT Services | Phones | Security

Most bizarre hacks:

- Hackers gained access to Target's network by infiltrating a [small HVAC company](#) and stealing that company's access credentials to Target's network.
- Hackers acquired data from a North American casino by using an [Internet-connected fish tank](#) thermometer. Hackers got into the fish tank and used it to move around into other areas of the network and sent out 10GB of data to a device in Finland.
- A man engaged in a [social engineering campaign](#) to hack into the Washtenaw County Jail's computer system. His goal was to modify prisoner records to get an inmate released early.
- Hackers in Austria [locked all the doors](#) to the Austrian Romantik Seehotel Jägerwirt hotel's electronic lock system so that guests couldn't get in their rooms. The hackers demanded a ransom to unlock the guests' rooms.
- Hackers got into an American university's network and caused more than 5,000 internet-connected objects on its campus to [continually search for the keyword "seafood."](#) This made the internet connection throughout the entire school almost come to a standstill because of the DoS attack.
- Hackers got into more than [800,000 smart teddy bears](#) created by CloudPets, which resulted in thousands of audio recordings from families being compromised.



BTS TECHNOLOGIES

IT Services | Phones | Security



03

SMBs like yours

Cyberattacks on small businesses are growing. In fact, they represent the largest share of all the attacks on organizations - 43% to be exact, according to the [yearly Verizon report](#) on Cybersecurity for 2019. Verizon also mentions that no business is too small, or too large for that matter, to fall victim to an attack. They also have found no correlation to a specific industry or vertical. The 43% of targeted small businesses suggests that no one is off limits.



BTS TECHNOLOGIES

IT Services | Phones | Security



Efficient Services Escrow Group of Irvine, California

The small Californian escrow firm was victim of a cyberheist and lost \$1.5 million dollars. The attackers got access to their networks through a remote trojan. Then, a wire for \$432,215 was made to an account in Russia, and two other wires totaling \$1.1 million were sent to accounts in the Heilongjiang province in China a month later. Three months after the first attack, the company was shut down and the staff of 9 people were laid off.

<https://www.itnews.com.au/news/15m-cyber-heist-causes-escrow-firm-to-close-its-doors-352902>



BTS TECHNOLOGIES

IT Services | Phones | Security



Patco of Sanford, Maine

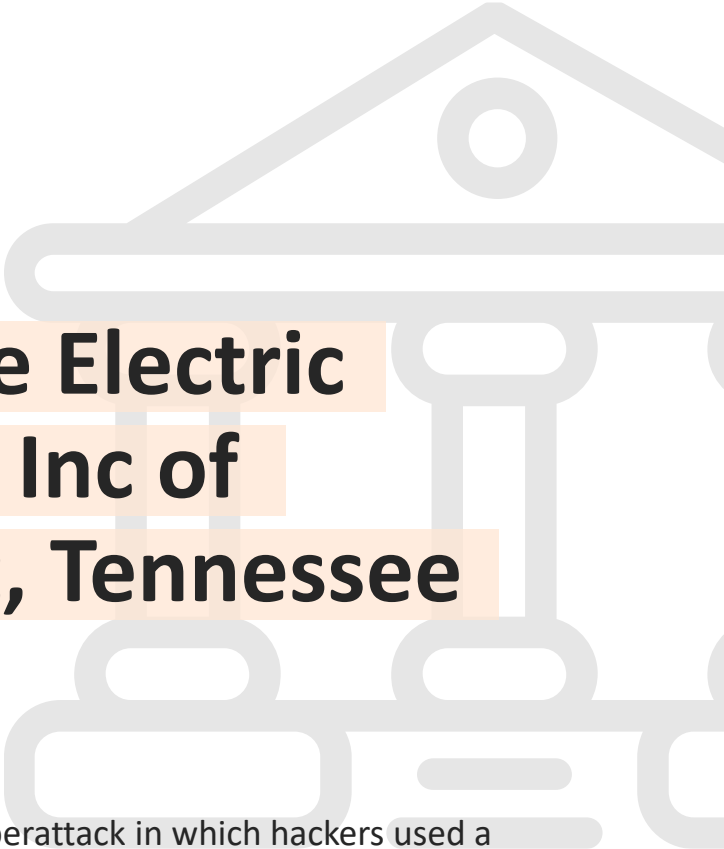
Using the Zeus password-stealing trojan on an employee's computer, hackers were able to access Patco's banking credentials. A social engineering attack allowed the cyber thieves to initiate a series of money transfers. Close to \$600,000 worth of transfers were made via six transactions before the organization took notice of what happened. Their bank, after being notified of what happened, was able to block close to \$240,000 in transfers, but Patco was unable to retrieve the rest.

<https://www.wired.com/2012/11/bank-to-pay-hacking-victim/>



BTS TECHNOLOGIES

IT Services | Phones | Security



Tennessee Electric Company Inc of Kingsport, Tennessee

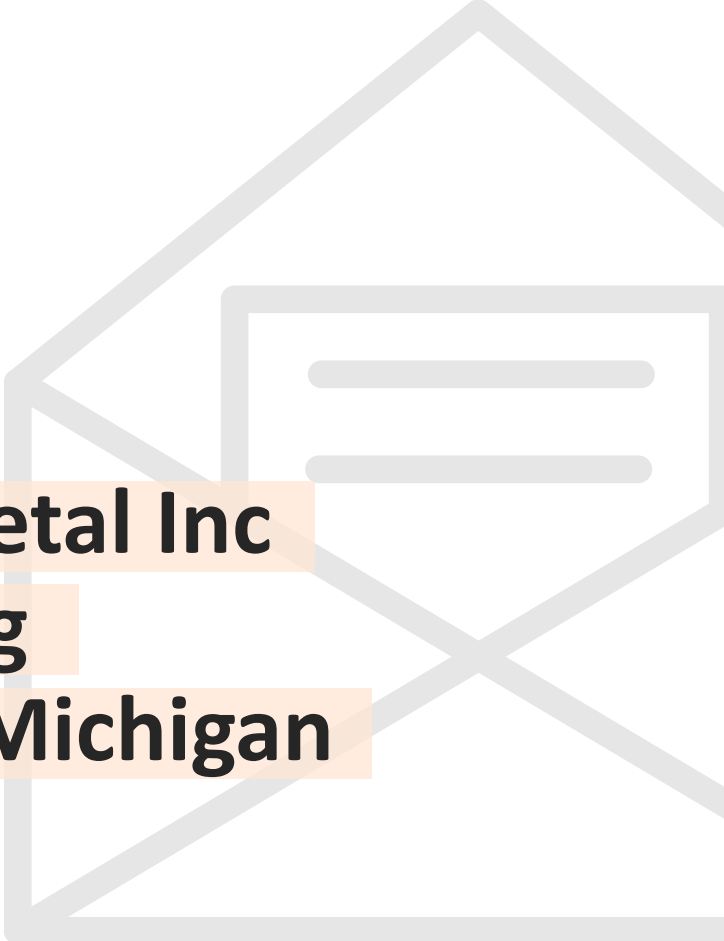
The company was the target of a cyberattack in which hackers used a network of money mules to store away money taken from their corporate account. The hackers likely gained access to TEC's bank account via password-stealing malware. The cyber thieves managed to siphon \$327,804 out of the company's accounts. TriSummit Bank was able to recover roughly \$135,000, leaving TEC with a loss of \$192,656.

<https://krebsonsecurity.com/2014/08/tenn-utility-sues-bank-over-327k-cyberheist/>



BTS TECHNOLOGIES

IT Services | Phones | Security



Experi-Metal Inc of Sterling Heights, Michigan

Using social engineering techniques, hackers sent an email to a company controller. The emailed looked like it was coming from their bank and asked the controller to log into their bank portal – a fake one – to renew the business’s digital certificate. Later, almost 100 wire transfers were performed within a few hours and managed to send roughly \$560,000 to bank accounts in China, Estonia, Finland, Russia and Scotland.

<https://krebsonsecurity.com/2011/06/court-favors-small-business-in-ebanking-fraud-case/>



BTS TECHNOLOGIES

IT Services | Phones | Security



Niles Nursing Inc. of Niles, Illinois

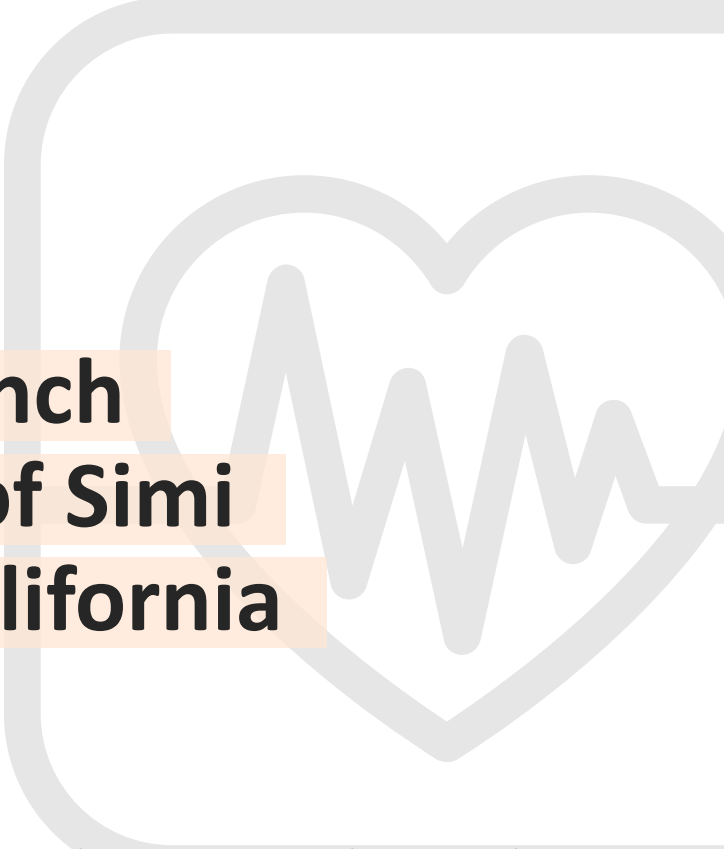
Once again gaining access to a controller's credential, online crooks logged into Niles Nursing Inc.'s online banking accounts and found their way into his hacked PC. The cyber thieves added money mules to the nursing home's payroll and were sent automated clearing house payments, totaling more than \$58,000. Those transfers were then withdrawn in cash and wired to individuals in Ukraine and Russia.

<https://www.nextgov.com/cybersecurity/2013/01/authorized-use-user-privileges-stolen/142891/>



BTS TECHNOLOGIES

IT Services | Phones | Security



Wood Ranch Medical of Simi Valley, California

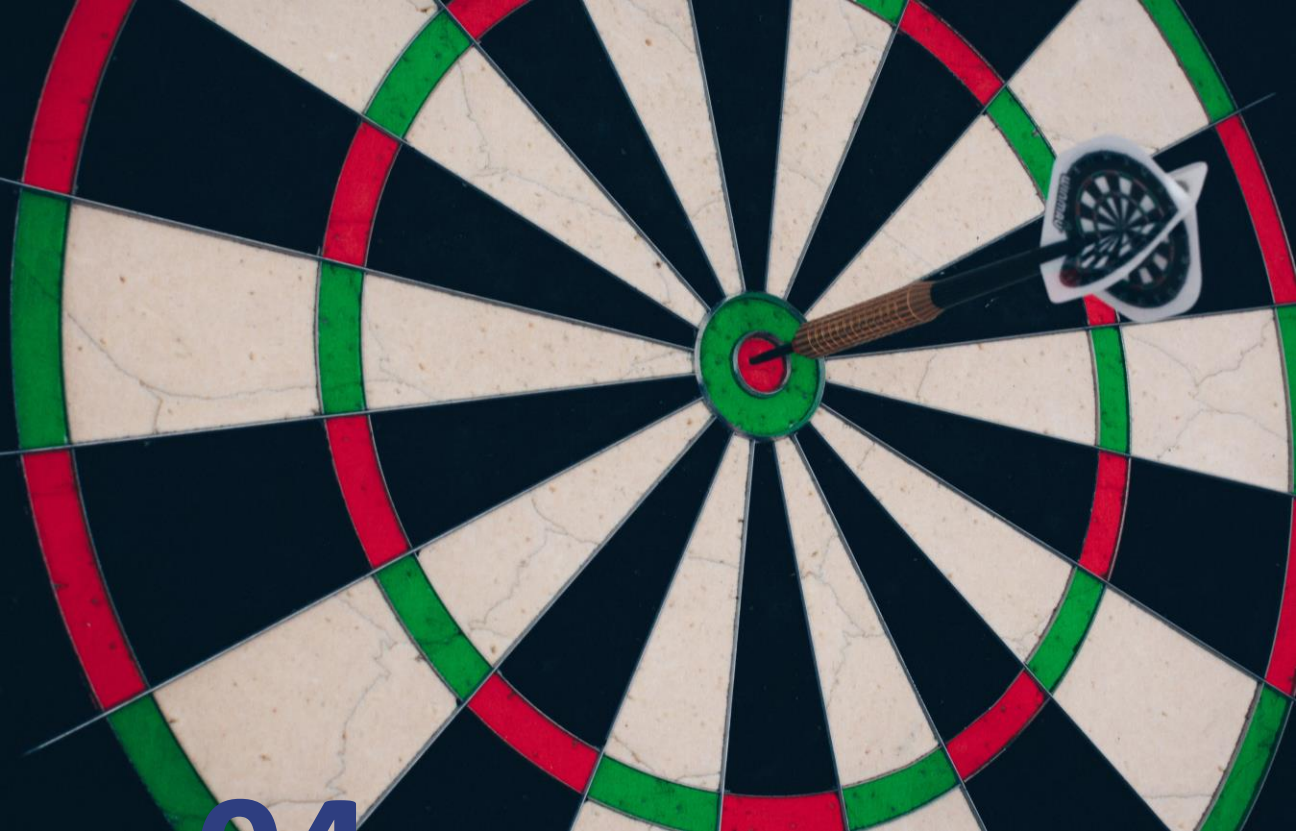
The attack infected the clinic's servers with ransomware. Cybercriminals caused widespread file encryption, as well as prevented medical records from being accessed. The computer systems were permanently damaged, making file recovery impossible. The practice also had backups of patient records, but they were also encrypted and could not be used to restore patient data. The incident affects 5,835 patients and led to the closure of the practice.

<https://www.hipaajournal.com/wood-ranch-medical-announces-permanent-closure-due-to-ransomware-attack/>



BTS TECHNOLOGIES

IT Services | Phones | Security



04

Why hackers target SMBs



BTS TECHNOLOGIES

IT Services | Phones | Security

55% of SMBs say they
don't have the budget to
combat cyber risks

<https://www.prnewswire.com/news-releases/nearly-70-percent-of-smbs-experience-cyber-attacks-half-do-not-know-how-to-protect-their-companies-300749965.html>



BTS TECHNOLOGIES

IT Services | Phones | Security

62% of SMB respondents
said that their firms don't
have an up-to-date or active
cybersecurity strategy--or
any strategy at all

<https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html>



BTS TECHNOLOGIES

IT Services | Phones | Security

Only 9% of small businesses rank cybersecurity as a top business priority. In fact, 18% rank cybersecurity as their lowest priority

<https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/>



BTS TECHNOLOGIES

IT Services | Phones | Security



05

What can you do?



BTS TECHNOLOGIES

IT Services | Phones | Security

Social engineering

Learn to spot scams, and teach your workforce to do the same.

Smarter password

Each password needs to be a unique string of 13 or more characters. Using a password manager will help.

Authentication

Enabling multi-factor authentication will keep unwanted users to access your accounts without having access to your smartphone.

Hire a professional

Buy peace of mind by letting managed service providers optimize your assets for a secure environment. They also provide 24/7 monitoring, as well as business continuity and disaster recovery scenarios.



BTS TECHNOLOGIES

IT Services | Phones | Security

Better security tomorrow starts with
a phone call today.

(205) 290-8400

Contact@askbts.com

Or schedule a consultation

