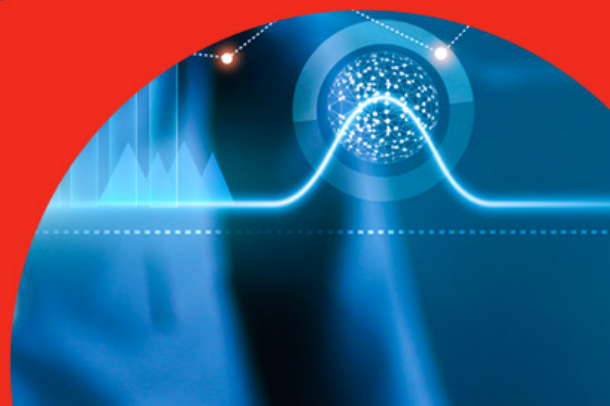




How to Stay Ahead of Cybercriminals in Financial Services

Prevent Attacks, and Secure Assets
with Automated Security Validation



01 | Living on the Edge

As long as there have been banks, thieves have been trying to make illegal withdrawals. And while the days of blowing open a bank safe or robbing the mail coach have long passed, criminals continue to follow a simple formula: follow the money. They have just gotten a lot smarter at how to go about it.

In today's digital world, managing and moving money have never been easier for consumers and corporations. Whether authorizing payment of supplier invoices, or paying bills through a bank's website, or buying a cup of coffee using a smartphone, digital services have made buying and selling more effortless than ever before. Even international money transfers are straightforward and near-instantaneous. The global monetary system has become much more efficient, as well as much more accessible. While making use of financial services has become simpler, the number of access points to such a firm's network has increased simultaneously, creating new avenues for cybercriminals to use as the entry point of an attack.

Branch offices have become a common source of new criminal attack vectors. With the explosion in networked IoT devices—from networked music systems to branch WiFi networks to networked security cameras—new access points become available to criminals. The increase in access points makes the job of end-to-end bank security extremely complex, essentially combining a bank's security needs with those of a retail outlet.

ATMs have been and remain a frequent target of organized cybercrime. ATM networks are frequently outsourced, with many terminals running outdated, vulnerable software that has not been upgraded to the latest security standards.¹ In a recent CISA (Cybersecurity and Infrastructure Security Agency) report,² US government investigators describe North Korea's systematic use of FASTCash malware on ATMs to commit large-scale theft—attacking ATMs in as many as 30 countries around the world simultaneously in one incident.

While this type of cybercrime tends to occur most commonly outside of the US, the use of ATMs as an entry point is a global vulnerability—yet another attack vector into a bank's central network. And once criminals have established a presence in a bank's network, they will use their landing point to gather information and credentials, moving laterally through the network over time to steal proprietary bank and client information that can be sold or used to commit other thefts.

Such attacks require careful planning: attackers often target specific individuals, and—unlike robbing the mail coach—today's thieves take their time, quietly exploring a target network for as long as a year before making a move.

However, the basic strategy for cybercriminals is known and straightforward: establish a foothold using a vulnerable endpoint, inject malware, create a covert command and control channel, move laterally through the network to find valuable data, and finally act (theft or ransomware). These attackers attempt to cover their tracks as they move—making detection more difficult—until they can gain access to the bank's central network, using credentials and privileges stolen along the way.

Finally, attackers look to use a target bank's internal processes to steal funds or confidential information. In a famous 2020 cyberattack, cybercriminals used the FASTCash malware to successfully breach the SWIFT network,³ which companies and banks use to send secure, authorized payments. By exploiting vulnerabilities in member banks' systems, hackers stole the banks' legitimate credentials, using them to send "trusted" messages authorizing fund transfers.

¹ WIRED Magazine, "ATM Hackers Have Picked Up Some Clever New Tricks," 08/15/2020,

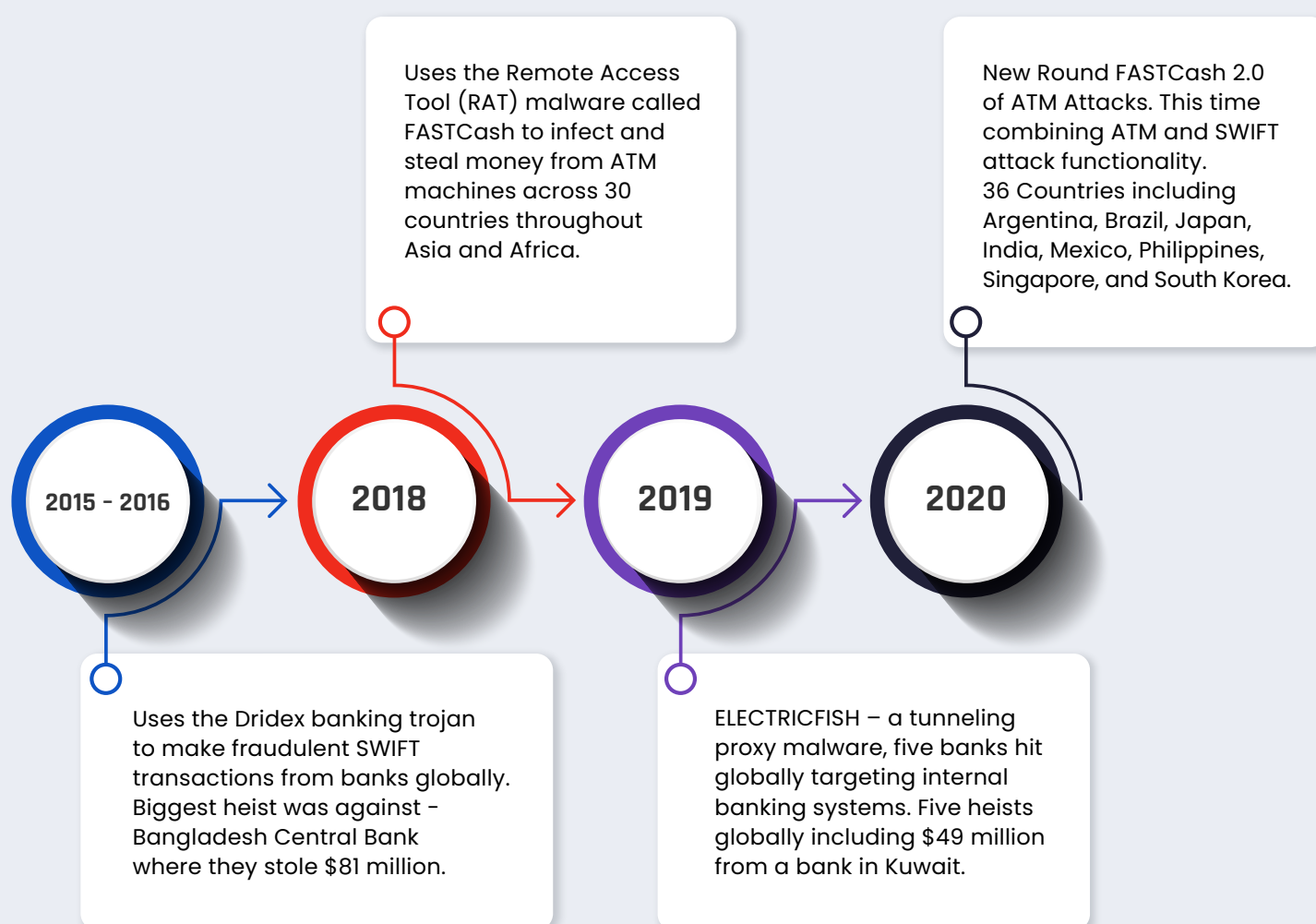
² CISA, "FASTCash 2.0: North Korea's BeagleBoys Robbing Banks, 08/26/20, <https://us-cert.cisa.gov/ncas/alerts/aa20-239a>

³ Bank Infosecurity Magazine "North Korean Hackers Tied to \$100 Million in SWIFT Fraud," 10/04/20, <https://www.bankinfosecurity.com/north-korean-hackers-tied-to-100-million-in-swift-fraud-a-11579>

02 | A Look at North Korea's Bank

Targeting APT 38 / Lazarus Group

This North Korean state-run attacker has a long history of infamous attacks. By far their biggest ongoing targets are banks and financial institutions worldwide. To date, they have stolen approximately over \$2 billion USD.



APT 39/Lazarus Timeline of Banking Attacks

Banks and other financial services firms are, of course, all too aware that they are prime targets for cybercrime, and as a result, have built some of the most secure networks in the world. Given that their security must protect a wide range of devices, financial services security is highly sophisticated and extremely complex. However, even with the best technology available, regular network changes and emergent threats can result in security drift, exposing or creating new, exploitable vulnerabilities.

03 | Stopping Attacks Before Payload Deployment

To remain secure in an environment of constant change, financial services and other highly targeted industries have implemented security assurance programs. These programs are designed to validate that network security is working as intended. Specifically, a thorough security assurance program should meet the following criteria:



Reveal new threat opportunities immediately to prevent potential access to your core network.



Scan for and identify the newest malware to halt or identify novel attacks as soon as possible.



Ensure proper policy enforcement is always in place: verify that correct authorization and access policies are followed. This not only prevents lateral movement but slows attackers down as they try to move through the network.



Supply prompt assurance: a network is a living thing, changing daily or hourly. Only frequent validation of network integrity and immediate detection of any potential breach can stop an attack before thieves can access valuable data.



Verify that configuration changes are performed correctly to prevent configuration errors from opening a door to criminals.

Today's standard practice for security validation consists of four well-defined processes: Security Audits, Vulnerability Scans, Pen Tests, and Red Team Exercises. If performed regularly, these methods help the security team evaluate and validate their network architecture and performance. However, while valuable and necessary, these tests alone are not sufficient: they cannot confirm that a security architecture will always work as designed. They cannot supply the real-time visibility, validation, and assurance needed to know if your security infrastructure is at its best state at any given moment. If testing frequency cannot keep up with the rate of change (internal or external), your network is vulnerable during the "gaps" between tests.

04 | Living on the Edge

Expand Current Security Assurance Program to Include Automated Breach and Attack Simulation

The most practical and effective way for a security team to test their network's security against malicious attacks is to use automated attack simulations that mimic the modes of attack used by the criminals themselves. These kinds of simulations are known as Breach and Attack Simulations (BAS). By combining frequent BAS tests with existing security testing methodologies, a security team can build a security assurance program that can keep up with the constant changes needed in their network while also assuring their system can defend against the latest threats.

Regular BAS testing reduces any exposure caused by security drift during "gaps" between standard tests, delivering tangible benefits that increase overall security effectiveness. Because BAS tests are automated, they can be run at any time, supplying the coverage and frequency of testing needed to stay ahead of cybercriminals in the continually changing threat landscape. In addition to performing your standard battery of security assurance testing, we recommend adding four types of automated BAS tests at frequent intervals:

01

Policy Enforcement Validation:

Policies and configurations change along with the network. This form of validation verifies policy enforcement across the entire system, examining access controls, the configuration of new IoT device security controls, user-onboarding policies, and unexpected effects of network maintenance. This test also confirms policy enforcement due to any internal IT changes. For example, this test verifies that the correct network segmentation policies are in place, preventing access between classified networks and non-classified networks, such as a guest WiFi network

02

Security Control Validation:

This test subjects security controls to a broad spectrum of attacks and threats. It validates the efficacy of data loss prevention (DLP) and endpoint security controls and supplies guidance for optimizing them. Whether installing new users, new endpoints, or new security equipment, this test assures that changes in your network do not inadvertently open new avenues of attack.

03

Threat Intelligence-Based Testing:

Cybercriminals never sleep. A vital part of any security assurance program requires validation testing against novel threats. This test allows you to stay abreast of the latest attack vectors and methods, prove your ability to prevent new attacks, and expose any vulnerabilities caused by these threats. This test gives you real-time visibility into the state of security against cybercriminals, optimizes your security controls against new threats, and tests overall security integrity, letting you stay ahead of the latest attacks before the criminals deploy them against you.

05

Purple Team Automation:

Purple Team Automation enables security teams to craft and launch attack flows to exercise threat hunting and incident response capabilities. Automation makes Purple Team exercises accessible and achievable for security teams with minimal adversarial skills by leveraging out-of-the-box attack scenarios. Sophisticated customizability enables companies with existing red team or pen tester experience to increase productivity by leveraging automation without limiting their creativity.

05 | Conclusion

Constant Vigilance Required to Maintain Security

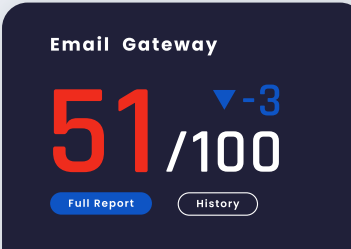
As the late 2020 breach of US Government networks by what the FBI believes to be a Russian government hacking group4 demonstrates, even what should be the most secure networks are not immune from penetration. In a digital world of constant change, new services, devices, and access points to networks create a threat landscape that is by nature unstable and unpredictable. As cybercriminals become more sophisticated, suppliers of security equipment and their customers face a never-ending battle against thieves and other bad actors.

Banks and financial services firms face an incredibly daunting task as they strive to protect themselves and their customers. Not only are financial organizations high-value targets, but the nature of the banking industry creates more inherent security risks, with banks sharing risk-profiles of both centralized corporate networks and distributed retail

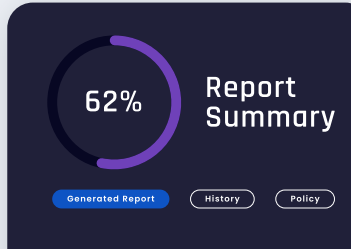
chains. Protecting any global network is a complicated and costly endeavor. By implementing a security assurance program that includes automated BAS testing at regular and frequent intervals, the security team can prevent, or at least quickly expose, even the most complex and sophisticated attacks. When defining a security assurance program, the guiding principle must be one of constant vigilance. Security teams should use automated tests that mimic real-life attack scenarios and run them in response to the rate of change in the internal or external environment. Automated BAS testing is the best and most practical way of keeping pace with today's rate of change and the growth of cybercrime. To learn more about the Cymulate BAS platform and how to build a more effective security assurance program, visit. www.cymulate.com.



1 Simulate
Simulate attacks across any vector.



2 Evaluate
Know where your company is exposed.



3 Remediate
Fix your security gaps.

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate continuously enhances its methods to prepare organizations for any attack scenario or campaign. With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness. **Measuring your cybersecurity performance is fundamental towards creating a more secure organization!**

Contact us for a live demo, or get started with a free trial

[Start Your Free Trial](#)