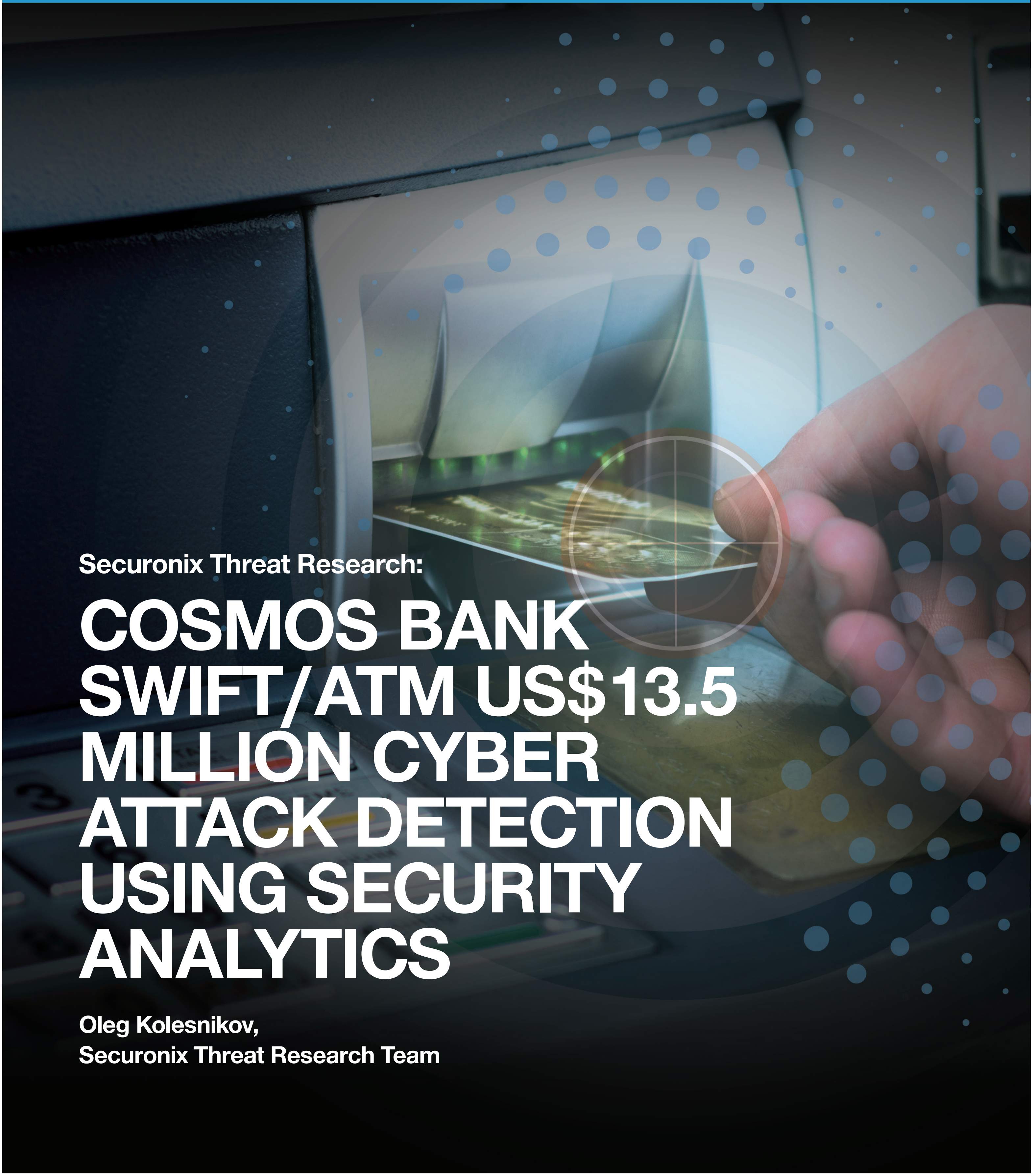
SECURONIX™
Security Analytics. Delivered.



Securonix Threat Research:

COSMOS BANK SWIFT/ATM US$13.5 MILLION CYBER ATTACK DETECTION USING SECURITY ANALYTICS

Oleg Kolesnikov,
Securonix Threat Research Team

Figure 1: Cosmos Bank in India US$13.5 Million SWIFT/ATM Cyber Attack of August 2018 [1]

Introduction

The Securonix Threat Research team recently learned of a new high-profile cyber attack targeting SWIFT/ATM infrastructure of Cosmos Bank (COSDINBB), a 112-year old cooperative bank in India and the second largest in the country, resulting in over US$13.5 million stolen [1,2].

Below is a summary of what we currently know about this high-profile attack and recommended Securonix predictive indicators and security analytics to increase your chances of detecting such attacks targeting financial services/SWIFT.

Summary

Impact

US$13.5 million stolen from Cosmos Bank between August 10-13, 2018.

Scope

Malware infection, ATM switch compromise, SWIFT environment compromise.

Attack Techniques

Multiple (see below).

Initial infiltration

Unconfirmed. Based on the attribution, likely spear phishing and/or remote administration/third-party interface.

Attribution

As of August 27, 2018: Currently attributed to a nation-state-sponsored malicious threat actor (Lazarus Group) by some sources [3,4]. Updated August 29, 2018: According to the latest report from the Maharashtra Special Investigation Team performing the investigation of the attack, they have not yet been able to link the attacks to the Lazarus or Cobalt hacking groups, noting that the Cosmos bank attackers “wiped out all tracks, leaving no evidence; it’s well-planned.” [5]. The latter is consistent with the behavior of major hacking groups, including Lazarus group, that are known to use tools that wipe out all tracks and evidence. To illustrate, according to the TrendMicro report on Lazarus Group operations from earlier this year, Lazarus Group use wiper tools that remove Prefetch, event logs, MFT records and other evidence from the compromised systems [6]. Updated October 2, 2018: The US-CERT AR18-275A HiddenCobra FASTCash report released on October 2, 2018 is consistent with the original attribution of this attack to the Lazarus/HiddenCobra malicious threat actor [7].

Cosmos Bank Attacks – Securonix Technical Analysis

While many technical details of the attack are currently unknown, based on publicly available details, our technical analysis, and expertise, here are some of the key technical details describing the most likely progression of this high-profile ATM/SWIFT banking attack:

Cosmos Bank Cyberattack – ATM Modality – US$11.5 Million Stolen:

- Following an earlier patient-zero compromise and lateral movement, on August 10-11, 2018, the bank’s internal and ATM infrastructure was compromised. The exploit involved multiple targeted malware infections followed by leveraging a set of malicious ISO8583 libraries and process code injections standing up a to stand up a malicious ATM/ POS switch (malicious-Central or MC) in parallel with the existing Central and then selectively breaking the connection between the Central and the backend/Core Banking System (CBS).

- After making adjustments to the target account balances to enable withdrawals, MC was then likely used in fake off-us, on-us, foreign-to-EFT, standing-in, etc. activity that enabled the malicious threat actor to authorize specific primary account number (PANs) transactions to implement ATM withdrawals for over US$11.5 million in 2849 domestic (Rupay) and 12,000 international (Visa) transactions using 450 cloned (non-EMV) debit cards in 28 countries.
- Using MC, attackers were likely able to send fake Transaction Reply (TRE)-/ISO8583 x210 messages in response to Transaction Request (TRQ) messages from cardholders and terminals. As a result, the required ISO 8583 messages (e.g. x200), were never forwarded to the backend/CBS from the ATM/POS switching solution that was compromised, which enabled the malicious withdrawals and impacted the fraud detection capabilities on the banking backend.

Cosmos Bank Cyberattack – SWIFT Modality – US$2 Million Stolen

On August 13, 2018, the malicious threat actor continued the attack against Cosmos Bank likely by moving laterally and using the Cosmos bank's SWIFT SAA environment LSO/RSO compromise/authentication to send three malicious MT103 to ALM Trading Limited at Hang Seng Bank in Hong Kong amounting to around US$2 million.

The ATM/POS banking switch that was compromised in the Cosmos Bank attack is a component that typically provides hosted ATM/POS terminal support, an interface to core banking solution (CBS) or another core financial system, and connectivity to regional, national or international networks. The primary purpose of the system is to perform transaction processing and routing decisions (see Figure 2)

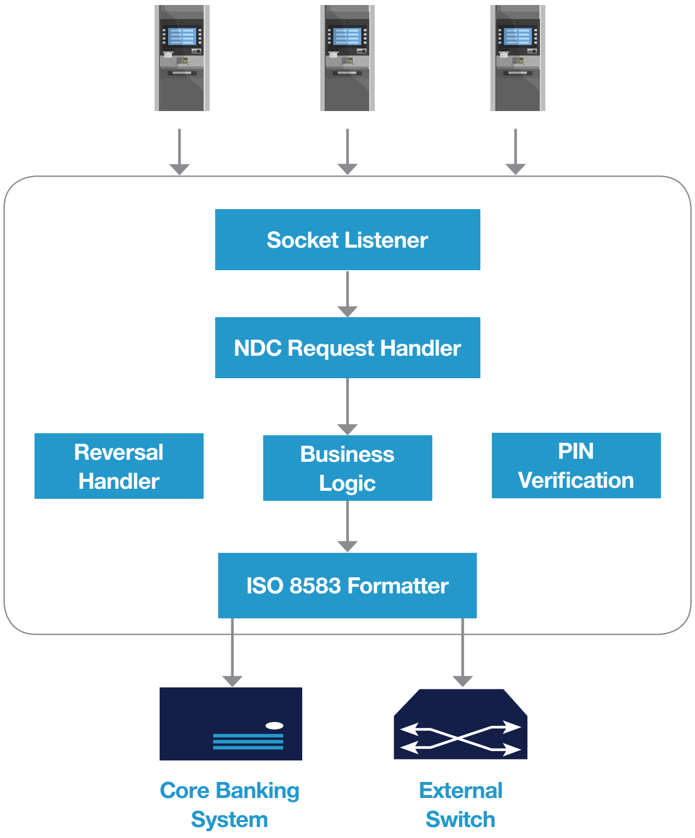


Figure 2: Common Banking ATM Switch Architecture

In case of the Cosmos Bank attack, this was not the typical basic card-not-present (CNP), jackpotting, or blackboxing fraud. The attack was a more advanced, well-planned, and highly-coordinated operation that focused on the bank's infrastructure, effectively bypassing the three main layers of defense per Interpol Banking/ATM attack mitigation guidance (see https://www.ncr.com/content/dam/ncrcom/content-type/brochures/EuroPol_Guidance-Recommendations-ATM-logical-attacks.pdf).

Based on our experience with real-world attacks involving ATM and SWIFT, following the initial compromise, attackers most likely either leveraged the vendor ATM test software and/or made changes to/injected into the currently deployed ATM payment switch software to effectively create a malicious proxy switch.

As a result, the details sent from payment switch to authorize transaction were never forwarded to CBS so the checks on PAN, card number, card status (Cold, Warm, Hot), PIN, and more were never performed. Instead, the request was handled by the MC deployed by the attackers sending fake responses authorizing transactions. Updated October 2, 2018: According to the latest details [7], this likely happened by modifying the checkPan() transport layer function functions and leveraging the GenerateResponseTransaction{1,2}().

In addition to the ATM and SWIFT monitoring, this attack likely involved a significant number of common cyber attack behaviors while the required malicious infrastructure needed to execute the attack was developed and stood up. As mentioned, this high-profile SWIFT/ATM banking attack is currently attributed to Lazarus Group/nation-state-sponsored actor/DPRK. Specifically some of the attack techniques commonly used by the threat actor include: use of Windows Admin Shares for Lateral Movement, using custom Command and Control (C2) that mimics TLS, adding new services on targets for Persistence, Windows Firewall changes, Timestomping, Reflective DLL Injection, and a number of other techniques (see https://attack.mitre.org/wiki/Group/G0032 for more details).Based on the details above, this attack is a good example of the fact that, while ATM and SWIFT transaction monitoring is important, it often is not enough, and may only give you 10-20% of the required detection coverage. In order to detect modern threat actors targeting banks, in addition to automatically baselining transactions, it is critical to also have the ability to monitor and baseline the behavior of your users, your systems, and your networks to detect anomalies (often 70-80%+ of success), and then connect all of the dots properly to detect an attack in progress.

Detection - Sample Spotter Search Queries

Updated October 2, 2018: Below are some sample trivial Spotter search queries to assist with detecting the existing malicious implants reported as part of the FASTCash/HiddenCobra/Lazarus Group attacks by US-CERT that was associated with Lazarus/HiddenCobra by FBI with high confidence [7].

ETDR Process Monitoring (Process Hash Conditions)

(rg_category contains “Endpoint” OR rg_category contains “ips” OR rg_category contains “ids”) AND (customstring3 = 10ac312c8dd02e417dd24d53c99525c29d74dcbc84730351ad7a4e0a4b1a0eba or
customstring3 = 3a5ba44f140821849de2d82d5a137c3bb5a736130dddb86b296d94e6b421594c or
customstring3 = 4a740227eeb82c20286d9c112ef95f0c1380d0e90ffb39fc75c8456db4f60756 or
customstring3 = 820ca1903a30516263d630c7c08f2b95f7b65dffceb21129c51c9e21cf9551c6 or
customstring3 = a9bc09a17d55fc790568ac864e3885434a43c33834551e027adb1896a463aafc or
customstring3 = ab88f12f0a30b4601dc26dbae57646efb77d5c6382fb25522c529437e5428629 or
customstring3 = ca9ab48d293cc84092e8db8f0ca99cb155b30c61d32a1da7cd3687de454fe86c or
customstring3 = d465637518024262c063f4a82d799a4e40ff3381014972f24ea18bc23c3b27ee or
customstring3 = f3e521996c85c0cdb2bfb3a0fd91eb03e25ba6feef2ba3a1da844f1b17278dd2)

Network Traffic/Proxy/Firewall (Outbound Conditions)

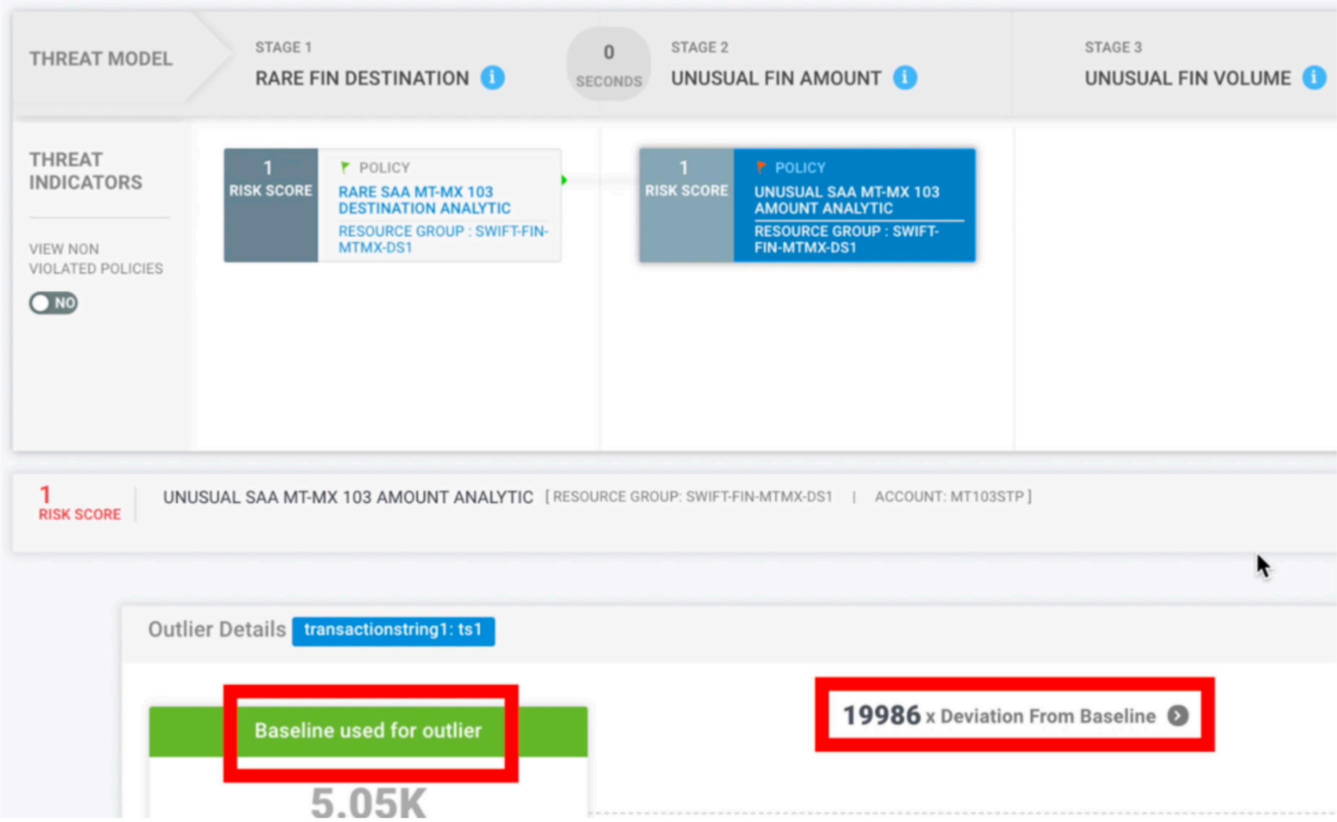
(rg_category = “Proxy” OR rg_category = “Firewall”) AND (destinationaddress = 75.99.63.27)

Detection – Securonix Behavior Analytics/Security Analytics

Based on the publicly available details available about the Cosmos Bank attacks, proper visibility into the environment (both from the endpoint and network perspective) as well as the ability to enrich and connect anomalies across different entities (users, frontend, backend, jump servers, third-parties, SWIFT, SAG, and more) was most likely key to be able to detect this attack.

Taking into account our expertise and the known techniques used by the threat actors attributed to the attack, particularly Lazarus Group, some high-level examples of the relevant Securonix behavior analytics/predictive indicators that could help detect such attacks in your banking environment include:

- Suspicious Process Activity - Targeted – Frontend and backend Transaction Discrepancy Analytic (This can be used to help detect malware activity utilized to compromise ATM switches e.g. where TR enters a payment switch but never leaves for authorization etc.)
- Suspicious Transaction Activity - 8583 x2xx F39 - Peak Unsuccessful Financial Responses Analytic (This can be used as a backup analytic to help detect malware activity involving proxy/injected MC failing to block initial PAN financial requests messages sent to the issuer.)
- Suspicious SWIFT Endpoint Activity - Rare SAA Process/MD5 Analytic
- Suspicious SWIFT Activity - Amount – Unusual 103 For Source Analytic
- Suspicious ATM Activity - Peak Sequential Non-EMV Transactions For ATM Source Analytic
- Suspicious Network Activity – Amount – Unusual PCCR Changes Analytic (This can be used to help detect unusual changes in the behavior of the ATM switches from a network perspective.)
- Suspicious ATM Activity – Peak EMV Fallbacks to Magstripe Analytic



THREAT MODEL

STAGE 1
RARE FIN DESTINATION

0
SECONDS

STAGE 2
UNUSUAL FIN AMOUNT

STAGE 3
UNUSUAL FIN VOLUME

THREAT INDICATORS

VIEW NON VIOLATED POLICIES
NO

1 RISK SCORE
POLICY
RARE SAA MT-MX 103 DESTINATION ANALYTIC
RESOURCE GROUP : SWIFT-FIN-MTMX-DS1

1 RISK SCORE
POLICY
UNUSUAL SAA MT-MX 103 AMOUNT ANALYTIC
RESOURCE GROUP : SWIFT-FIN-MTMX-DS1

1 RISK SCORE
UNUSUAL SAA MT-MX 103 AMOUNT ANALYTIC [RESOURCE GROUP: SWIFT-FIN-MTMX-DS1 | ACCOUNT: MT103STP]

Outlier Details transactionstring1: ts1

Baseline used for outlier
5.05K

19986 x Deviation From Baseline

Figure 3: Example of Securonix Detecting Advanced Banking/SWIFT Cyber Attacks In Practice Using Security Analytics

- Suspicious Network Activity – Rare Outbound Network Connection For Host Analytic (This can be used to help detect attack activity associated with the compromised ATM switch.)
- Suspicious ATM Activity – Peak *On-Us Transaction Volume For PAN Analytic

- Suspicious ATM Activity – Amount – Unusual Foreign Cash-out Volume Analytic
- Suspicious Transaction Activity – Targeted – Cash Withdrawal Limit Elimination Analytic – Malicious threat actors manually changing cash withdrawal limits
- Suspicious Process Activity – Rare Scheduled Task For Host Analytic (This is an example that can be used to detect one of the common techniques leveraged by Lazarus Group to which the attacks were attributed.)
- Suspicious Process Activity – Targeted – Executable File Creation Analytic
- Suspicious Network Activity - Targeted - New Firewall Rule Created For Host Analytic

References

[1] Gitesh Shelke. Cosmos Bank Data From 9 Years Compromised. Times of India. 19 August 2018. https://timesofindia.indiatimes.com/city/pune/cosmos-bank-data-from-9-years-compromised-in-rs-94-42cr-heist/articleshow/65456374.cms.
Last Accessed: August 20, 2018

[2] Penny Crossman. An ATM attack the FBI warned of came to pass. Expect more. American Banker. 22 August 2018. https://www.americanbanker.com/news/an-atm-attack-the-fbi-warned-of-came-to-pass-expect-more?feed=00000158-babc-dda9-adfa-fefef5720000. Last Accessed: August 22, 2018

[3] Graeme Burton. ATM hackers steal $13.5m in 28 countries from India’s Cosmos Bank – just days after FBI warning. 15 August 2018. https://www.computing.co.uk/ctg/news/3061187/atm-hackers-steal-usd135m-in-28-countries-from-indias-cosmos-bank-just-days-after-fbi-warning. Last Accessed: August 28, 2018

[4] ET Online. North Korean connection to Cosmos hacking? Signs point to Bangladesh heist masterminds. 15 August 2018. https://economictimes.indiatimes.com/industry/banking/finance/banking/north-korean-connection-to-cosmos-hacking-signs-point-to-bangladesh-heist-masterminds/articleshow/65411640.cms.
Last Accessed: August 28, 2018

[5] Geetha Nandikotkur. Information Security Media Group. Cosmos Bank Heist: No Evidence Major Hacking Group Involved. August 29, 2018. https://www.inforisktoday.in/cosmos-bank-heist-no-evidence-major-hacking-group-involved-a-11435.
Last Accessed: August 28, 2018

[6] Trend Micro. A Look into the Lazarus Group's Operations. January 24, 2018. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations. Last Accessed: August 28, 2018

[7] US-CERT. Alert (TA18-275A)–HIDDEN COBRA – FASTCash Campaign. 2 October 2018. https://www.us-cert.gov/ncas/alerts/TA18-275A. Last accessed: October 3, 2018.

SECURONIX

ABOUT SECURONIX

Securonix is radically transforming all areas of data security with actionable security intelligence. Our purpose-built, advanced security analytics technology mines, enriches, analyzes, scores and visualizes customer data into actionable intelligence on the highest risk threats from within and outside their environment. Using signature-less anomaly detection techniques that track users, account and system behavior, Securonix is able to detect the most advanced insider threats, data security and fraud attacks automatically and accurately.

CONTACT SECURONIX

www.securonix.com
info@securonix.com | (310) 641-1000

1018

SECURONIX™

Security Analytics. Delivered.