



beSTORM

beSTORM は、製品がリリースまたは展開される前にそのセキュリティを確保するためのインテリジェントなブラックボックスファザーです。効率性、柔軟性、広範性といった、テストチームに共通する優先事項に対応するように設計されています。独自の優先順位アルゴリズムを使用して、最も高い確率の脆弱性から自動的に攻撃を開始し、選択されたプロトコルに対して数十億の攻撃を段階的に展開します。これらのプロトコルは既知、拡張、独自または未知のものです。

beSTORM は、ほとんどユーザーの介入を必要とせずにこのテストを実行します。テスト対象のシステム外部にセットアップできるので、複数のプロセッサやマシンを使えばテスト時間が大幅に短縮されます。異常や脆弱性を自動的に記録し、テストを継続し、最終的にチーム全体でそれらの情報を共有し、セキュリティ対応に有効で実行可能なレポートを生成します。

動的テストソリューション

- **言語に依存しない:**

beSTORM は、バイナリアプリケーションをテストすることで数十億の攻撃を実行します。使用されるプログラミング言語やシステムライブラリに全く依存しません。

- **スケーラブル:**

beSTORM は、通信範囲全体をテストします。これにより、大規模で複雑なコードベースを持つ製品にも無理なく対応できます。

- **柔軟性:**

beSTORM は、ソースコードとの相互作用を必要としません。このため、ソースコードにアクセスできないチームも beSTORM からエクスポートされたテストを使用することができます。

未知の脆弱性の発見

静的コードツールは、既知の脆弱性に関する特定のケーススタディやシナリオに基づいて、数千から数万のテストを実行します。これは、過去に知られている攻撃から製品を防御し、強化することに相当します。しかし、beSTORM は通信範囲全体にわたって数百万、場合によっては数十億の攻撃組み合わせを実行します。これにより、既知の過去の攻撃だけでなく、将来発生する可能性のある未知の攻撃に対しても製品をテストします。

包括的

beSTORM は、既知のプロトコルだけでなく、拡張、独自、新規プロトコルも迅速に学習してテストすることができます。すべての通信標準（SIP などの複雑な標準を含む）およびレベル（ネットワーク、プロトコル、ファイル、ハードウェア、DLL、API）にわたって動作します。beSTORM は、すべての可能な入力組み合わせを徹底的に検索して、入力実装の弱点をテストします。これらのテスト中には強力なモニターが動作し、システムがクラッシュしなくても、わずかなバッファオーバーフロー、フォーマット文字列またはメモリエクセプションが発生した場合に将来の攻撃を検出して通知します。

柔軟性

beSTORM は、独自または拡張プロトコルの分析をサポートします。beSTORM が独自または拡張プロトコルに遭遇すると、自動学習機能がこれをログに記録し、このプロトコルに対するテストの構築および拡張を開始します。これらの入力タイプは、beSTORM がキャプチャしたネットワークトラフィック、他の手段でキャプチャされたネットワークトラフィックを含むファイルサンプル、または API を記述する構文である可能性があります。beSTORM はこれらのデータセットを使用して、プロトコルやファイルがどのように構築されているかを判断します。完全な仕様が利用可能な場合、ユーザーは XML エディタを使用して beSTORM モジュールを作成または拡張することもできます。

また、beSTORM では、技術的な RFC ドキュメントで使用される BNF 記述を攻撃言語に変換して、プロトコル標準テキストを自動化されたテストセットに変換することもできます。これにより、RFC ドキュメントまたは同等のものをアップロードするだけで、新しい通信標準に即時対応、実行が可能です。

実行可能なレポート

beSTORM は、修正を目的として設計されています。そのため、beSTORM は、攻撃が成功した脆弱性について詳しく説明した、分かりやすく実行可能なレポートを提供します。beSTORM はケーススタディに対するテストではなく、テスト対象の製品に対して行動的に攻撃するため、ほとんどすべての偽陽性が排除され、包括的でクリーンなレポートがユーザーに提供されます。

発見された脆弱性は、アプリケーションのデバッグに使用できる詳細な脆弱性レポートとしてエクスポートできます。開発者は、beSTORM の使用方法を知らなくても、選択した開発環境内でこれらの脆弱性レポートをロードし、すぐにデバッグプロセスを開始できます。

システム要件

- **推奨要件:** クアッドコアプロセッサ (i5 以上) 、8GB の RAM (Windows 10) 、1GB の HDD 空き容量
- **最低要件:** x86-64 CPU、1GB の RAM (Linux、Docker、組み込みアプリケーション) 、250MB の HDD 空き容量

Basic

- DHCP Server (Simple)
- DNP3 - Master (Simple)
- DNP3 - Master Serial (Simple)
- DNP3 - Slave (Simple)
- DNP3 - Slave Serial (Simple)
- FTP Server (Simple)
- HTTP (Simple Web Client)
- HTTP Server (Simple Web Server)
- HTTPS Server (Simple Web Server)
- IEC61850 (MMS - Master - Simple)
- IEEE802.11 (AP - Simple)
- IEEE802.11 (Subscriber - Simple - UDP)
- IEEE802.11 (Subscriber - Simple)
- IMAP Server (Simple)
- Internet Printing Protocol (Simple)
- LLDP (Simple)
- Modbus (Master - Simple)
- Modbus (Master Serial - Simple)

- Session Initiation Protocol (Simple)
- SMTP Server (Simple)
- SNMP (Simple)
- SNMPv2 (Simple)
- SNMPv3 (Simple)
- SNMPv3 with MD5 (Simple)
- SNMPv3 with MD5 and DES (Simple)
- SNMPv3 with SHA1 (Simple)
- SSH Server (Simple)
- SSL Server (Simple)

Network / Client / TCP

- Border Gateway Protocol
- Common Industrial Protocol (EtherNet/IP)
- Diagnostic Over Internet Protocol
- Diameter
- DNP3 - Master (5Layers)
- EtherNet/IP
- FTP
- HTTP/1.0 (SSL Web Client)

- HTTP/1.0 (Web Client)
- HTTP/1.1 (SSL Web Client)
- HTTP/1.1 (Web Client)
- HTTPS (Simple Web Client)
- ICAP
- IEC60870-5-104 - Master
- IEC61850 (MMS - MAster)
- IMAP
- KIES
- LDAP
- MCAP
- Modbus (Master)
- MQTTv3
- Network Configuration v1.0
- Network Configuration v1.1
- NFS Client
- NNTP
- OPC Unified Architecture - Simple
- Open Network Video Interface Forum
- Open vSwitch Database Management
- OpenFlow Switch
- POP3
- RMI (Client)
- RSH
- RTSP
- SFTP Client
- SMB Client
- SMTP
- SOAP over HTTP
- SSH
- Telnet
- TLS v1.2 Client
- TLS v1.3 Client
- TPKT

Network / Client / UDP

- IEEE802.11 (AP)
- IEEE802.11 (Subscriber)
- Advanced Audio Distribution Profile
- Alternate MAC/PHY
- AMQP

- ATT
- BFD Control
- BVLC
- COAP
- DHCP
- DNP3 - Master
- DNS
- DNS (Simple)
- Dropbox LAN Sync Discovery
- DVMRP
- EtherCAT over UDP
- Fastboot
- GTPv1
- HDCPv1.1
- HDCPv2.0
- HSU
- ISAKMP
- ISUP
- L2CAP
- Label Distribution Protocol (Simple)
- LLC
- LLMNR
- NAT-PMP
- NTP
- OBEX
- Portmap Client
- RADIUS
- Real-time Transport Protocol (with Register)
- Real-time Transport Protocol (without Register)
- RFCOMM
- RIPng
- RIPv1
- RTP Control Protocol
- Service Discovery Protocol
- Service Location Protocol
- Session Description Protocol
- Session Initiation Protocol
- Session Initiation Protocol (with Register)
- Simple Service Discovery Protocol
- STUN

- Syslog
- TAPA
- Teredo
- TFTP
- URB
- USB Mass Storage
- USB Request Block

Network / Server-side

- DNP3 - Slave
- DNS Server (Simple)
- IEC60870-5-104 - Slave
- IEC61850 (MMS - Slave)
- Modbus (Slave)
- NTP Server
- OpenFlow Controller

Low-level Network

- ISIS
- MPLS LDP
- OSPFv2
- OSPFv3
- AllJoyn
- ARP
- Cisco Discovery Protocol
- Cisco Group Management Protocol
- EtherCAT
- Ethernet
- Generic Routing Encapsulation
- GOOSE
- HSRP
- HSRPv2
- ICMPv4
- ICMPv6
- ICMPv6 (ND)
- IEEE802.1Q
- IGMPv0
- IGMPv1
- IGMPv2
- IGMPv3
- IPsec AH

- IPv4
- IPv6
- IPv6 (SHIM6)
- Layer 2 Tunneling Protocol
- Link Layer Discovery Protocol
- Locator/ID Separation Protocol
- PIMv2
- PPPoE
- PROFINET PTC
- PROFINET RT
- PROFINET RT DCP
- RGMP
- SCTP
- STP (Spanning Tree Protocol)
- TCPv4
- TCPv6
- UDPlite
- UDPv4
- UDPv6
- VRRP

File

- ANI
- AVI (H264 -AC3)
- AVI (XVID)
- BMP
- DOC
- GIF
- HTML
- HWP
- ICO
- JASC-PAL
- JPEG
- MKV
- MP3
- MP4
- MPEG4
- PAL
- PCAP
- PDF
- PNG

- PPT
- TGA
- TIFF
- UPX
- WAV (PCM)
- WMV
- XLS

EDSA

- EDSAv2-401 Ethernet
- EDSAv2-402 ARP
- EDSAv2-403 IPv4
- EDSAv2-404 ICMPv4
- EDSAv2-405 UDPv4
- EDSAv2-406 TCPv4
- EDSAv3-401 Ethernet
- EDSAv3-402 ARP
- EDSAv3-403 IPv4
- EDSAv3-404 ICMPv4
- EDSAv3-405 UDPv4
- EDSAv3-406 TCPv4

Bluetooth / Bluetooth LE

- GAP
- GATT
- Hands free protocol
- HID over BT
- HID over GATT
- iBeacon
- Running Speed and Cadence

Serial

- DNP3 - Master Serial
- DNP3 - Slave Serial
- IEC60870-5-101 - Master
- IEC60870-5-101 - Slave
- Modbus (Master Serial)
- Modbus (Slave Serial)
- Modbus ASCII (Master Serial)
- Modbus RTU (Master Serial)
- Zigbee

Automotive

- CANBUS
- CANBUS (Over ICS)
- CANBUS (Over PCAN)
- CG4579 (Over PCAN)
- J1939-21
- OBDII
- OBDII (Over ICS)
- OBDII (Over PCAN)
- Unified Diagnostics Services TCPv4
- UDS (Over PCAN)

Custom Development Module (独自プロトコルの試験、自動的学習・テストケース生成、および独自プロトコルの構築用)

- TCPv4
- UDPv4

お問い合わせ

株式会社ユビキタス AI エンベデッド第三事業部

<https://www.ubiquitous-ai.com/contact/feel-free/>