

Renaud Bidou

Radware



BLACK HAT BRIEFINGS

A Dirty BlackMail DoS Story

This is a real story of modern extortion in a cyberworld. Bots have replaced dynamite and you don't buy "protection" to prevent your shop from going in flames; you buy "consulting" to prevent your IT from being DoSed. From the first limited synflood to the conclusion, we will review those crazy 48 hours that end up in a one to one digital fight. We will see in depth which attacks and mitigation techniques were involved and how they both evolved quickly in complexity and intensity. As a conclusion we will see which were the major weaknesses, found either in the network architecture, the security perimeter and the target application, and how it would have been possible to prevent such attack, limit its impact... and save money.

Renaud Bidou has been working in the field of IT security for about 10 years. He first performed consulting missions for telcos, pen-tests and post-mortem audits, and designed several security architectures. In 2000 he built the first operational Security Operation Center in France which quickly became the 4th French CERT and member of the FIRST. He then joined Radware as the security expert for Europe, handling high criticality security cases.


In the mean time Renaud is an active member of the rstack team and the French Honeynet Project with studies on honeynet containment, honeypot farms and network traffic analysis. He regularly publishes research articles in the French security magazine MISC and teaches in several universities in France.




 A Dirty Blackmail Story

rstack.org

Renaud BIDOU
renaudb@radware.com



Context



Context | The Target

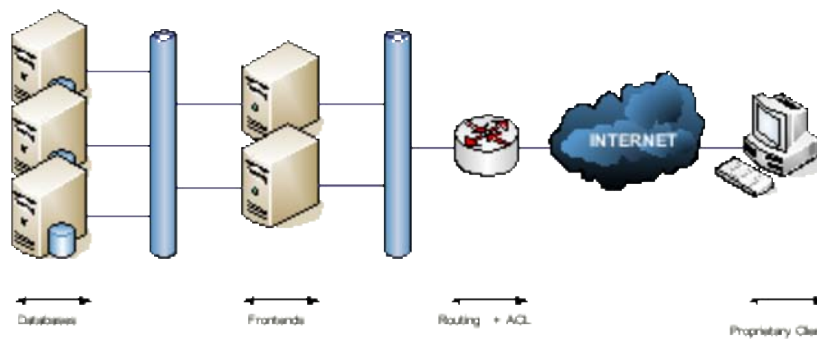
- Russian Company
 - Based in Moscow
 - Financial business
 - Performs change transactions
- DoS Exposure
 - Proprietary application
 - Client-side application for customers
 - 100% of business is made on-line

The Perfect Target



rstack.org

Context | Architecture



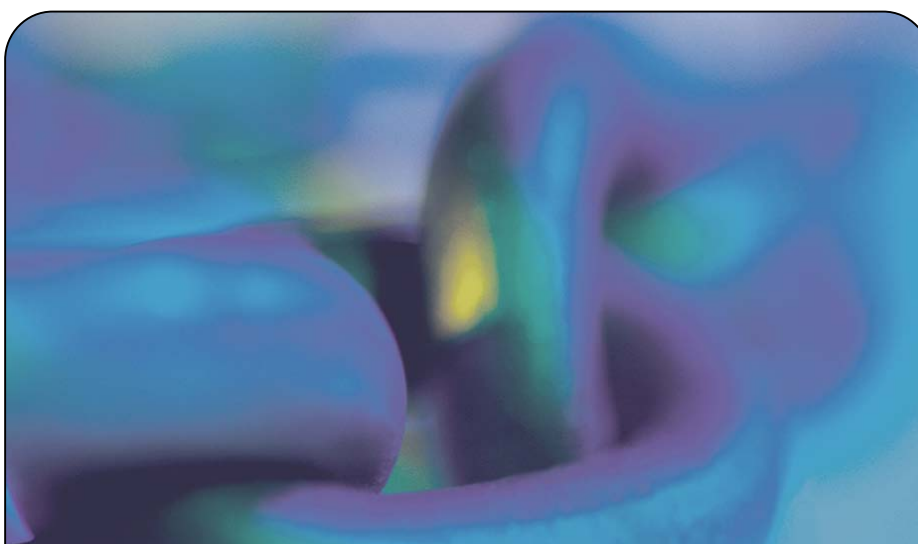
rstack.org

Context | Frontend operations

- Functional aspects
 - User authentication
 - Request formatting
 - Formatted requests are forwarded to DB servers
- Technical aspects
 - On top of high TCP port
 - All transactions are encrypted
 - Proprietary encryption
 - Paranoia = No more information available at this point



rstack.org



First Wave



Extortion



rstack.org

Extortion | The alert

- t0
 - Misbehavior identified
 - Frontend servers are freezed
 - No more connection possible
 - Very high router CPU utilization
 - t0 + 15 mn
 - Network traffic analyzed
 - Different sources, 1 target IP and port
 - Only SYNs (around 150.000 per second)
- SYNFlood



rstack.org

Extortion | Blackmail

- t0 + 30 mn
 - Contact via ICQ
 - X M\$ dollards must be paid
 - Before t1 = t0 + 36h
 - Howto kept secret by the target
- t0 + 60 mn
 - SYNflood stopped



rstack.org

Against SYNfloods



rstack.org

Protection | Client Side

- SYN_cookies
 - Session TCP established on behalf of the server
 - SYN/ACK sequence number calculated
 - $\text{SYN_ACK_SEQ} = f(\text{net_params.time})$
 - TCB => CPU tradeoff
 - Sequence numbers not to be guessed
 - $f()$: hashing function
 - $\text{SYN_ACK_SEQ} = f(\text{seed.net_params.time})$
- Setup
 - As close as possible from the resource to protect



rstack.org

Protection | Telco Side

- Protecting against spoofing
 - uRPF (*Unicast Reverse Path Forwarding*)
 - Strict : Packets are blocked if destination network is not part of the FIB (*Forwarding Information Base*) of ingress interface.
 - Loose : Packets are blocked if source is not part of the RIB (*Routing Information Base*) of the router (RFC 1918, reserved address etc.)
 - VRF (*Virtual Routing and Forwarding*)
 - Provides to uRPF a routing table per eBGP session.
- Setup
 - uRPF strict : Customer / ISP edge
 - uRPF loose : ISP / ISP edge
 - uRPF strict + VRF : ISP / ISP edge



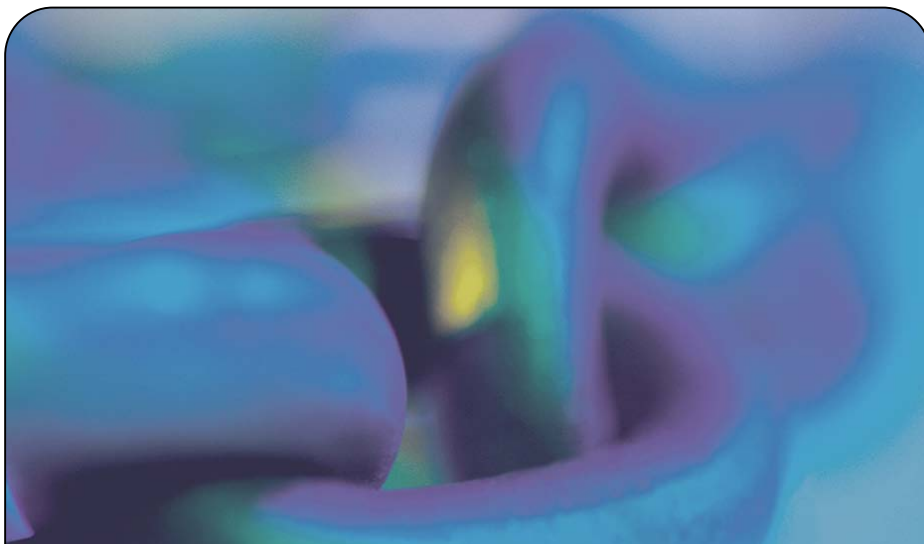
rstack.org

Protection | Telco Infrastructure

- Save willy
 - BHR setup (Black Hole Routing)
 - Defining a static routing rule toward a specific IP to null0 (express forwarding, no impact on performances).
 - Sending a BGP Send : Next-hop to the target = @IP routed to null0
 - No packet to reach the target
 - DoS is successful
 - Infrastructure is safe
 - No impact on the telco
 - Other systems stay up and running



rstack.org



Prelude
Before the tempest



Prelude | 36 hours

- **Issues**
 - BHR is not acceptable
 - No solution to can be implemented on a telco infrastructure in 36 hours
 - **Analyze**
 - Spoofed source
 - No way to setup ACL
 - High target port, no previous scan identified
 - Attacker knows the application
 - May have a copy of the proprietary client application
- Application level attacks to be expected



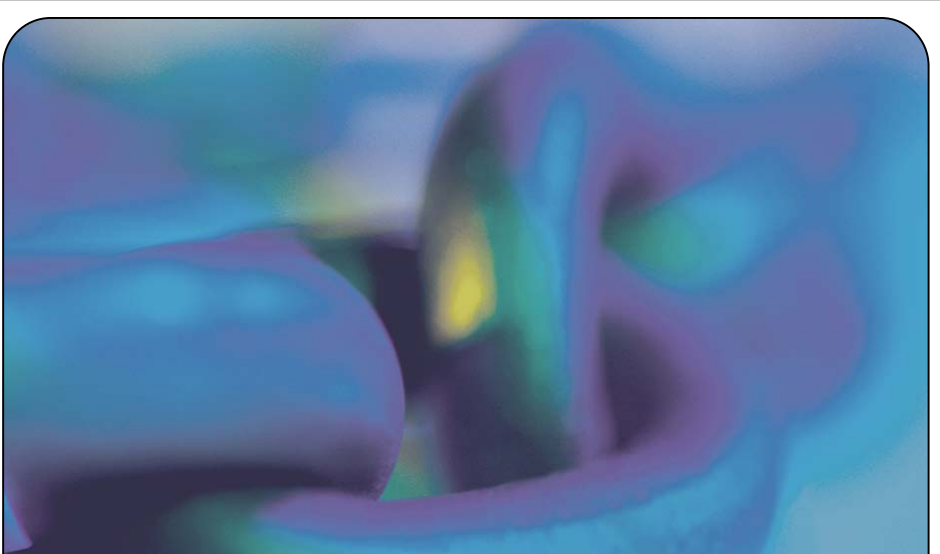
rstack.org

Prelude | Day 0 Defense


- **Immediate protection**
 - Provide SYNCookies for frontends
 - Setup a real stateful firewall
 - Clean link to the firewall to save CPU resources
- **Limits**
 - Internet access router
 - Will hardly handle more than 150.000 pps
 - No support from ISP
 - Traffic will arrive unfiltered
 - ISP infrastructure may be hit



rstack.org



Second Wave



Network level attacks



Network | SYN Flood II

- Operating mode
 - $t1 = t0 + 36h$
 - Same as SYN Flood at $t0$
 - Power increasing by steps
 - $t1 + 5 mn = 50.000 pps$
 - $t1 + 10 mn = 100.000 pps$
 - $t1 + 15 mn = 150.000 pps$
- Successfully blocked by SYN Cookies



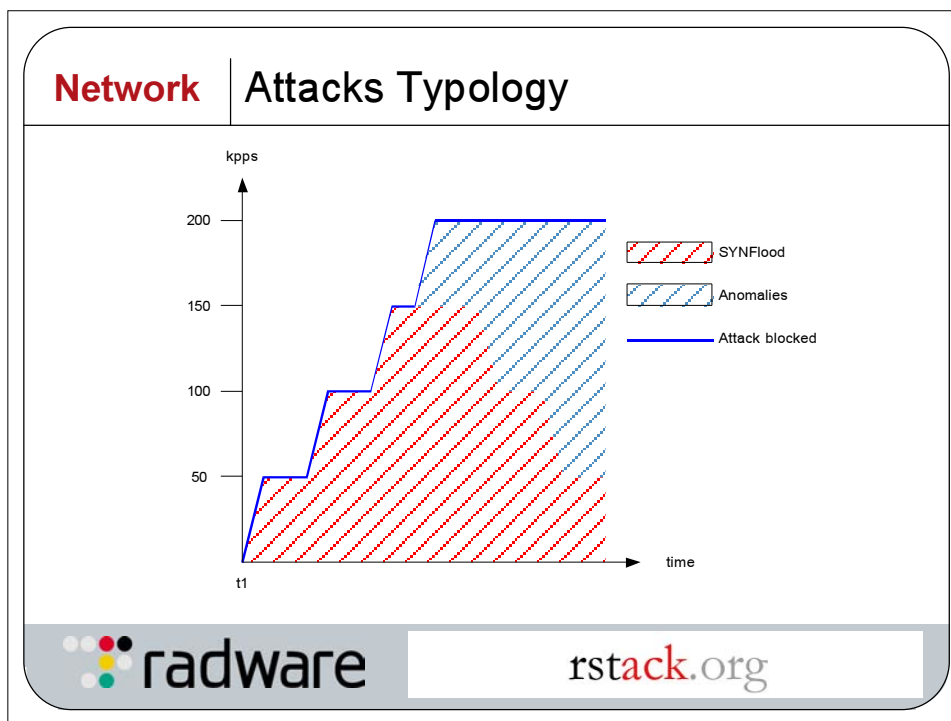
rstack.org

Network | Protocol anomalies

- New attack
 - New traffic typology
 - $t1 + 20 mn = SYN 150 kpps / Anomalies 50 kpps$
 - $t1 + 25 mn = SYN 100 kpps / Anomalies 100 kpps$
 - $t1 + 30 mn = SYN 50 kpps / Anomalies 150 kpps$
 - Anomalies
 - Xmas Tree with sequence number = 0
 - Land
 - SYN/ACK (reflection attack)



rstack.org



- ## Network | Anomaly DoS handling
- Detection techniques
 - Per packet signature
 - Too many signatures * packets
 - Sampling
 - 1 packet out of n analyzed
 - Heuristics
 - Detection of traffic out of a standard pattern
 - Blocking
 - Rely on stateful engines
 - Too many packets
 - Inline with sampling/signature or heuristics
 - Suspicious traffic redirected to a "washing machine"
 - Only bad traffic redirected to inline device
- radware rstack.org

Application level





Application Pending sessions

- t1 + 35 mn
 - Legitimate connections established
 - 1st data packet with random payload

Freeze of connection at 5.000 sessions/s
- Mitigation
 - Need to understand the application
 - 1st data packet payload starts with \00\01

Stateful inspection
SYN - SYN/ACK - ACK - ACK (\00\01)



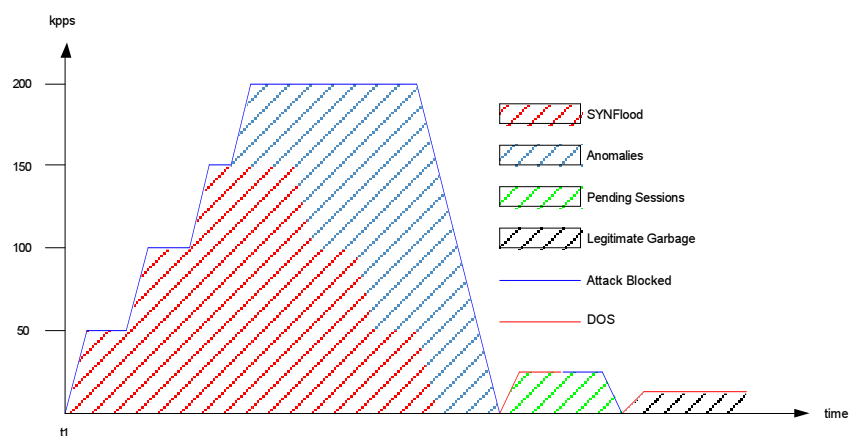
Application | The insider

- New application level attack
 - SYN - SYN/ACK - ACK - ACK (100\01 + random data)
Crash at the 1st session established
 - Overflow somewhere I guess
 - We need to know more but ...
 - Paranoia = no access to system, no dumps
 - Application developed by political prisoners who died in Siberia 5 years ago (or something like that)
- Then ...
 - It is a dirty blackmail story



rstack.org

Application | Attack Typology



rstack.org



Conclusion



Conclusion | Source analysis

- Botnets
 - Probably 4 of them
 - Maybe command-line relays
 - All attacks could have been performed by hping3
 - Specific flexible application
- The attacker
 - Knew how the application works
 - Tried other attacks first
 - Spoofed not to reveal IP of bots
 - Application independant not to reveal its knowledge of the target application



rstack.org

Conclusion | We were lucky

- Limited number of users
 - We could create large blacklists of IP ranges
 - Dirty but the only efficient way to block
- Just a question of time
 - Attacker did not insist, probably afraid of getting caught
- Security is a process, but...
 - You still need a brain
 - Paranoia has limitations
 - As well as security by obscurity
 - If you don't want to trust anybody : do it by yourself



rstack.org

Questions ?



rstack.org

