Lotan differs from traditional approaches by not relying on signature-based techniques or IP whitelisting for detection, but rather uses automated static and dynamic analysis of application crash dumps to identify security threats. Without the use of an agent, Lotan redirects application crash dumps to its cloud analysis platform, instead of other vendor services. The R&D team targeted memory corruption exploits based on observed trends in memory corruption exploits such as increased frequency and severity (CVSS³). This approach is interesting due to two properties of memory corruption attacks:

First, exploits are fragile in the face of heterogeneity – no adversary can possibly test for all target configurations, thus exploitation success depends on a predictable target. In addition to the complexity introduced by varied targets, an attack must overcome modern exploit countermeasure technologies such as ASLR and DEP⁴. Secondly, memory corruption attacks introduce new code into the memory of the target process.

Modern hackers understand that exploitation is difficult and unreliable. Attackers assume that most of the time, their initial attacks will fail. What they did not assume until now, was exploit failures pinpoint what they attempted, how they attempted it, and where they are operating from. The remnants of a failed attack by their very nature contain both the payload and the vector used in the attack. Lotan is the best available tool that uses this information to detect sophisticated attacks and shorten the incidence response timeline.

1. A software agent is a computer program that acts for a user or other programs.
3. Common Vulnerability Scoring System
4. Address space layout randomization and Data execution prevention

1. A software agent is a computer program that acts for a user or other programs.
3. Common Vulnerability Scoring System
4. Address space layout randomization and Data execution prevention
Compatibility
Lotan is compatible with Windows Vista through Windows 10 (WER 2). After a simple registry change, Lotan can be up and running on your Enterprise Windows Environment in a matter of minutes. Linux-based hosts are compatible through the use of a kernel shim module, but requires additional configuration.

Lotan also supports out-of-the-box SIEM integration with Splunk, and all of Lotan’s analysis data is available through its REST API. To learn more about bespoke SIEM integration and specific Linux distribution consulting, see the section below.

Leviathan Consulting
Maintaining and operating third party software can be cumbersome. Leviathan’s security experts have a wide array of expertise to efficiently guide your IT support staff, saving you time and increasing the sophistication of your organization. Contact us today for more information on the following services:

→ Custom SIEM integrations
→ Shellcode analysis and reverse engineering
→ IT operations system analysis
→ On-site deployment consulting
→ Specific Linux distribution consulting
→ Product training

Quarterly and semi-annual in-depth reporting to answer these critical organization questions:

How secure am I?
Am I better off than I was this time last year/quarter?
Am I spending the right amount of money?
How do I compare to my peers?
What risk transfer options do I have?

About Leviathan
Leviathan was formed by the principals of @stake, Guardent, Symantec, and Foundstone when they decided to collaborate and combine the expertise from their decades of information security experience. Over the years, we have added research, education, and security strategy experts to expand our client offerings, training programs, and business structure.

The members of Leviathan Security Group are dedicated to integrated Risk Management and Information. Security solutions that are not just patches, point fixes, or checking off little boxes with red ink pens. Rather, our methodology helps our clients/governments to understand and mitigate their business and technology risks. We help them take the next steps in their evolution and help them maintain their stellar reputations.